(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 101375546 B
(45)授权公告日 2012.09.26

(21)申请号 200680023517.6

(22)申请日 2006.04.28

(30)优先权数据
60/676,141 2005.04.29 US

(85)PCT申请进入国家阶段日
2007.12.28

(86)PCT申请的申请数据
PCT/US2006/016085 2006.04.28

(87)PCT申请的公布数据
WO2006/118968 EN 2006.11.09

(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚州

(72)发明人 托马斯·埃曼努埃尔·瓦赫瑟
乔恩·布赖恩·费希尔
史蒂文·皮卡斯·哈里斯
唐·布斯科·迪瑞

(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 11038
代理人 袁玥

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
US 6263447 B1,2001.07.17, 全文.
US 5875296 A,1999.02.23, 全文.
US 2004/0117320 A1,2004.06.17, 全文.
US 6853973 B2,2005.02.08, 摘要, 说明书第1栏第14行到第44行, 第4栏第23行到第7栏第21行, 附图1-2.
US 6853973 B2,2005.02.08, 摘要, 说明书第1栏第14行到第44行, 第4栏第23行到第7栏第21行, 附图1-2.
US 2004/0215980 A1,2004.10.28, 说明书第28段到第51段, 附图3A,3B,4-5.
US 2004/0215980 A1,2004.10.28, 说明书第28段到第51段, 附图3A,3B,4-5.
US 2003/0097593 A1,2003.05.22, 全文.

审查员 曹晓宁

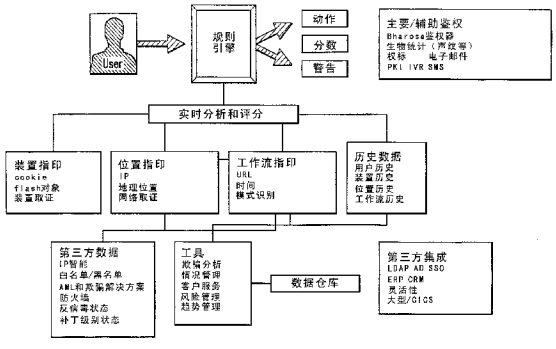
权利要求书 2 页 说明书 48 页 附图 19 页

(54)发明名称

用于欺骗监控、检测和分层用户鉴权的系统和方法

(57)摘要

本发明提供了用于通过呈现根据与所述装置相关联的所感知的欺骗风险选择的多个图形用户界面之一,对来自用户装置的访问请求进行鉴权的系统和方法。用户装置被使用指印信息识别,并且其相关联的欺骗风险是从对于所述装置或者对于类似装置的过去经验和从第三方信息确定的。在优选实施例中,根据欺骗风险和在已知用户的情况下的可用性来呈现不同的图形用户界面。在优选实施例中,本发明被实现为多个通信模块,其识别用户装置,估计它们的欺骗风险,呈现所选择的用户界面,并且维护欺骗经验的数据库。本发明还包括提供这些鉴权服务的系统。



CN 101375546 B

1. 一种用于对访问服务器的当前访问请求进行鉴权的方法，所述当前访问请求发起自网络连接的装置，所述方法包括：

收集关于发起所述当前访问请求的装置的识别信息；

从装置中央库DCR检索关于所述当前访问请求的风险信息，其中，所述DCR将关于欺骗请求的风险的历史风险信息与标识所述欺骗请求的发起装置的信息相关联地存储；

通过向包括所收集的识别信息和所检索的风险信息的信息应用规则来确定鉴权界面选择标准；

从具有各种安全性和/或可用性级别的多个鉴权界面中选择依赖于所确定的界面选择标准的鉴权界面，其中，所选择的鉴权界面的安全性和/或可用性对应于欺骗请求的风险；

在所述发起装置上呈现所选择的鉴权界面；

根据响应于所呈现的鉴权界面而在所述发起装置上输入的鉴权信息，将所述当前访问请求鉴权为有效或无效；

用当前风险信息更新存储在所述DCR中的历史风险信息，所述当前风险信息是通过向包括当前的访问请求的鉴权结果的信息应用规则而确定的，其中，所述被更新的历史风险信息是对应于所收集的识别信息的历史风险信息；以及

向所述服务器应用提供所述鉴权信息。

2. 按照权利要求1的方法，其中，所述当前访问请求包括登录或者执行金融交易的请求，其中，所收集的识别信息唯一地标识所述装置。

3. 按照权利要求1的方法，其中，所收集的识别信息还包括在所述发起装置上存储的永久数据。

4. 按照权利要求3的方法，还包括：

根据所收集的识别信息的至少一部分来组配装置ID数据项；并且

在所述发起装置上将所述装置ID数据项存储为永久数据。

5. 按照权利要求3的方法，其中，所述永久数据包括cookie或者受保护以防止变更的信息。

6. 按照权利要求1的方法，其中，所收集的识别信息还包括与所述发起装置的特性或者所述发起装置的网络连接的特性相关联的信息。

7. 按照权利要求6的方法，其中，所收集的装置特性包括下述的至少一个：通信适配器MAC地址、本地时间、本地时区、微处理器类型、微处理器处理特性、微处理器序号网络地址、网络连接速度、数据上载到服务器的网络速率或者从服务器的数据下载的网络速率。

8. 按照权利要求1的方法，其中，还根据所述当前访问请求的内容来确定所述界面选择标准。

9. 按照权利要求1的方法，其中，还根据来自一个或多个第三方数据提供者的另外的数据来确定所述界面选择标准。

10. 按照权利要求1的方法，其中，至少部分地根据来自一个或多个第三方提供者的数据，来评估欺骗请求的风险。

11. 按照权利要求10的方法，其中，所述第三方数据提供者包括装置地理位置数据提供者和/或装置黑名单数据提供者和/或装置白名单数据提供者。

12. 按照权利要求 1 的方法，其中，在所述 DCR 中存储的历史风险信息包括装置黑名单和装置白名单，其中，更新所述历史风险信息还包括：向包括从装置地理位置数据提供者和 / 或装置黑名单数据提供者和 / 或装置白名单数据提供者接收的数据的信息应用规则。

13. 按照权利要求 1 的方法，其中，所述应用规则的步骤还：

至少部分地根据所收集的识别信息来评估当前的访问请求是欺骗的风险；以及

至少部分地根据所评估的欺骗风险来确定界面选择标准。

14. 一种用于对访问服务器应用的当前访问请求进行鉴权的系统，所述当前访问请求发起自网络连接的装置，所述系统包括：

用于收集关于发起所述当前访问请求的装置的识别信息的装置；

用于从装置中央库 DCR 检索关于所述当前访问请求的风险信息的装置，其中所述 DCR 将关于欺骗请求的风险的历史风险信息与标识发起所述请求的装置的信息相关联地存储；

用于通过向包括所收集的识别信息和所检索的风险信息的信息应用规则来确定鉴权界面选择标准的装置；

用于从具有各种安全性和 / 或可用性级别的多个鉴权界面中选择依赖于所确定的界面选择标准的鉴权界面的装置，其中，所选择的鉴权界面的安全性和 / 或可用性对应于欺骗请求的风险；

用于在所述发起装置上呈现所选择的鉴权界面的装置；

用于根据响应于所呈现的鉴权界面在所述发起装置上输入的鉴权信息，将所述当前访问请求鉴权为有效或无效的装置；

用于用当前风险信息更新存储在所述 DCR 中的历史风险信息的装置，所述当前风险信息是通过向包括当前的访问请求的鉴权结果的信息应用规则而确定的，其中，所述被更新的历史风险信息是对应于所收集的识别信息的历史风险信息；以及

用于向所述服务器应用提供所述鉴权信息的装置。

15. 按照权利要求 14 的系统，其中，发起所述访问请求的所述网络连接的装置包括 PC 类型的计算机。

16. 按照权利要求 14 的系统，其中，发起所述访问请求的所述网络连接的装置包括用户终端。

17. 按照权利要求 14 的系统，其中，所述多个鉴权界面被存储在界面数据库中。

18. 按照权利要求 14 的系统，其中，在与执行所述服务器应用的处理器不同的处理器上执行下述内容的处理的一个或多个：收集、检索、确定、选择、呈现、鉴权、更新和提供。

19. 按照权利要求 14 的系统，其中，在与所述 DCR 远离的处理器上执行所述更新的处理。

20. 按照权利要求 14 的系统，其中，执行界面选择标准的确定还包括应用规则，所述规则编码了用于在服务器上对访问请求进行鉴权的要求。

21. 按照权利要求 20 的系统，其中应用规则还：

至少部分地根据所收集的识别信息来评估当前访问请求欺骗的风险；并且

至少部分地根据所评估的欺骗风险来确定界面选择标准。

22. 按照权利要求 14 的系统，还包括规则定义数据库，用于存储所应用的规则。

用于欺骗监控、检测和分层用户鉴权的系统和方法

技术领域

[0001] 本发明一般地涉及用于在计算机网络上提供对身份盗用的防御的系统和方法。

背景技术

[0002] 由企业和个人在因特网上进行的在线交易量的增长已经难以置信。敏感的私人身份信息通常用于对用户鉴权以进行在线交易。身份信息在因特网交易上的越来越多的使用已经伴随有该信息的截取和盗用的越来越多的危险。当某人未经同意使用另一个人的密码、用户名、社会安全号码、信用卡号码或者其他识别个人信息来进行欺骗时，发生身份盗用。按照 2003 年 9 月的联邦贸易委员会 (FTC) 调查，在过去 5 年中有 2730 万美国人成为身份盗用的受害者，其中包括在 2002 年一年中就有 990 万人。按照 FTC 的调查，在 2002 年中商业和金融机构的身份盗用损失总共达到近乎 480 亿美元，并且消费者受害者报告有实际现金支出 50 亿美元。

[0003] 为了进入与电子商务服务器的交易，用户通常需要提供敏感和保密的数据，其中包括鉴权数据，用于描述交易的数据等。通常通过使用用户的本地装置（其正在运行链接到因特网（或者其他计算机网络）的万维网浏览器）的键盘和 / 或鼠标来输入这个数据。图 1 是图解用于输入用户鉴权和交易数据的示例系统 10 的图。在这个示例中，由用户输入的鉴权信息包括用户 ID 和密码。在已知的系统中，用户 ID 和密码由在计算装置 14 上执行万维网浏览器时经由键盘 12 输入的字符串构成。由浏览器在显示器 16 上向用户提供的典型的用户输入界面 18 被示出。

[0004] 在输入后，用户的敏感信息通常最好以加密的形式通过安全连接被发送到远程服务器。例如，广泛使用的 TCP/IP 通信协议包括在加密套接字协议层 (SSL) 协议上建立的安全协议，以允许使用加密的数据流来传送安全数据。SSL 提供加密、源鉴权和接收完整性来作为用于保护在不安全的公共网络上交换的信息的手段。因此，许多电子商务服务器和应用使用 SSL 或者类似的安全协议来在远程服务器和本地用户系统之间交换数据。如果被输入的鉴权信息被服务器批准，则用户被允许从服务器的网站发送和接收数据。

[0005] 经常从发送消息的装置的 IP 地址和 / 或从来自用户的数据中包括的 cookie 来确定在万维网服务器接收的消息的源。cookie 一般表示由万维网服务器向在用户的计算机系统上驻留的浏览器发送的信息（经常是敏感信息）的包，用于保存到文件，并且用于每当用户的浏览器从服务器发出另外的请求时发回服务器。IP 地址一般被包括在消息首标中，cookie 通常是已经由服务器（经常是在登录时）预先发送的那个。服务器将用户登录数据与消息 IP 地址和返回的 cookie 相比较，以确定发送消息的用户的身份和是否用户当前已经登录到服务器中。用户的 IP 地址也被确认。

[0006] 虽然有这些已知的预防措施，用户的敏感信息仍然脆弱，因为其在远程发送之前在其由用户输入和其加密之间处于未经处理的不安全形式。而且，从服务器发送的敏感数据在其解密后直到其显示的时段期间是脆弱的。可以以多种方式来秘密地捕获这种不安全的信息。例如，cookie 截取者从 cookie 复制敏感信息。而且，键盘记录器和鼠标点击记录

器是隐藏的软件，其在用户输入之后但是在被浏览器或者其他软件处理之前截取和复制鼠标点击和按下的按键。记录器软件可以容易地截取用户的安全信息。键盘记录器和鼠标点击记录器也可能采取在键盘和鼠标电缆和计算机之间连接的硬件或者在键盘和鼠标装置内的硬件的形式。

[0007] 即使是表示具有用于用户输入的可选择图形（替代地或者另外地还提供用于文本输入的字段）的屏上小键盘和键盘的图形用户界面也容易受到鼠标点击记录器、屏幕捕获记录器和其他方案的伤害。图 1、2 和 3 图解了这样的界面的现有技术的示例。在图形界面中的每个字母数字字符被表示为唯一的图形图像，诸如形成数字“1”的像素。屏幕捕获记录器使用光学字符识别 (OCR) 技术来解密由鼠标点击选择的字符和对应的字母数字图形，以便确定用户的 ID 和密码的实际字母数字文本字符。复杂的屏幕捕获记录器也可以使用图形图像的校验和和大小特性，以便确定对应于在用户输入期间由用户的鼠标点击选择的图形图像的数据项。在这些方式中，即使当图形用户界面已经在小键盘或者键盘上重新布置了字母数字字符的顺序时，所述屏幕捕获记录器也可以获得个人信息。

[0008] 间谍软件（包括窥探软件、间谍软件、非病毒恶意软件、黑客工具、监视工具、木马等）也可以截取敏感信息。窥探软件有助于未经授权地获取关于个人或者组织的信息，而未经它们知道或者同意。其通常未经同意地将其本身安装在用户的计算机上，然后监控或者控制所述装置的使用。窥探软件可以捕获每个用户键击、所有的聊天会话、所有所访问的网站、用户与浏览器的每次交互、所执行的每个应用程序、所打印的每个文件、所有的文本和图像。窥探软件通常能够本地存储或者通过因特网向第三方发送所捕获的数据，经常是未经用户知道或者同意。

[0009] 敏感个人信息的另一个欺骗获取者是“在肩上的”(over-theshoulder) 间谍，其秘密地读取用户的显示器以获取信息。

[0010] 已知的反病毒和反间谍软件产品试图使得用户能够防御这样的恶意软件。但是，过期的反病毒和反间谍软件文件的使用最多提供了计算机数据对于外部威胁的最小保护。因此，这些产品的缺点是由反病毒和反间谍软件程序使用的信息必须不断被更新，以反映新发现的方案，以便将所述防御保持为最新的。除了将病毒信息保持为最新的，还必须定期对系统扫描可能的感染。

[0011] 而且，已知某些地理位置包含过多数量的身份盗窃者。因此，有益的是已知访问服务器的尝试来自何方。IP 地址是一种容易获得的位置信息。但是 IP 地址具有缺陷在于：对于许多用户，IP 地址不是不变的。已知的网络协议和设施会导致可变的 IP 地址。例如，代理服务器用于在组织的局域网和因特网之间提供网关。本地网络被安装在代理服务器上的防火墙软件保护。每次从用户装置发送新的消息时，代理服务器向所述用户装置动态地分配新的 IP 地址。结果，对于经由代理服务器连接到因特网的用户，不存在被分配到单独的用户装置的不变的 IP 地址。

[0012] IP 地址可变性的另一个来源是通常使用的动态主机配置协议 (DHCP 协议)，其动态地和自动地向在 TCP/IP 网络上的装置分配 IP 地址。当一个装置连接到网络时，DHCP 服务器从可用地址的列表中向所述装置分配一个 IP 地址。所述装置仅仅在当前的会话持续时间中保留这个 IP 地址。一些 DHCP 服务器系统可以在所述会话期间动态地改变用户的 IP 地址。代理或者 DHCP 服务器的使用表示所述 IP 地址本身可能不足以识别特定的用户装置。

[0013] 防御上述风险的安全系统和方法也应当满足一般用户的可用性问题。服务提供商希望以安全的方式来鼓励在线使用。但是，麻烦和冗长的用户界面或者用户不友好的界面可能使用户感到害怕或失望，或者引起用户出错等。而且，安全系统应当创立预防措施，以便一旦发现用户的信息和/或系统有被损害的风险则防止执行欺骗的交易。安全系统也应当基于试图与用户无关地访问提供商的系统的特定装置提醒服务提供商。

[0014] 而且，安全系统和方法应当使得服务提供商能够在系统的安全和可用性之间获得适当的平衡。换句话说，需要一种系统和方法来使得服务提供商能够当未识别安全风险时提供一种容易使用和较低安全性的界面，并且当识别了风险时提供较高安全性的界面。另外，期望的安全系统和方法应当尽可能少地依赖于人的动作来保持它们的安全状态。例如，无益的是要求用户保存和维护权标（token）或数字证书等。权标可能丢失、损坏、被盗等。

[0015] 但是，在本领域中一般不知道用于防御所述的威胁并且具有上述的特性的安全系统。在本领域中所需要的但是当前缺少的是具有下述特征和方面的安全系统和方法：

[0016] -是基于装置的欺骗监控系统；

[0017] -提供强壮的（robust）欺骗监控和检测以及强壮的欺骗分析和风险估计，以便在线服务提供商具有用于确定如何和是否允许装置访问提供商的系统所需要的实时信息；

[0018] -根据可用性和/或者安全性考虑来提供安全用户鉴权的可选择的级别；

[0019] -确定用户的信息和/或系统已经被损害的安全风险，如果如此，则提供更安全的登录界面以防御欺骗活动；

[0020] -可以与其他安全跟踪信息库合并的信息库，用于根据用户设备的更可靠和强壮的指印获取来识别合法和欺骗的用户；

[0021] -是不需要发行和维护硬件装置的纯基于软件的身份盗用解决方案；

[0022] -对于在线用户方便。

发明内容

[0023] 本发明的系统和方法通过提供改善的鉴权服务而填补了现有技术的空白。

[0024] 按照本发明的系统和方法的优点是它们提供信息和可选择的用户界面，用于使得服务提供商能根据由试图进行交易的用户和装置带来的风险来实时地采取行动以授权、拒绝或者挂起在线交易。

[0025] 本发明的另一个优点是其使得服务提供商能够根据用户和装置历史数据分析来识别可能的在处理中的（in-process）欺骗鉴权交易。可以根据一组预定规则来批准、拒绝或者挂起以验证多个交易。

[0026] 本发明的另一个优点是其提供了基于用户和装置的强壮欺骗监控和检测以及强壮的欺骗分析和风险评估，以向服务提供商提供用于确定如何和是否允许装置访问所述提供商的系统所需要的实时信息。

[0027] 本发明的另一个优点是使得能够根据预定的可用性和/或安全性来选择安全用户图形鉴权的级别。

[0028] 本发明的另一个优点是不依赖于权标、板卡或者其他类似的硬件装置、数字证书、反病毒软件或者个人防火墙解决方案来保护终端用户防止在线身份盗用。

[0029] 本发明的另一个优点是获取和开发基于装置而不是仅仅基于用户的黑名单和/

或白名单。

[0030] 广义而言，按照一个实施例，本发明通过获得可以用于估计由用户在用户装置处带来的欺骗风险的装置识别信息而对所述用户装置进行指印处理。按照另一个实施例，本发明执行与访问服务提供商的服务器的装置相关联的欺骗分析和风险警告。按照另一个实施例，本发明包括用户装置的数据库和在中央库中的它们的历史已知欺骗风险。按照另一个实施例，本发明提供了从提供多个级别的安全和可用性的多个用户鉴权界面中选择的用户鉴权界面。

[0031] 因此，本发明提供了用于提供欺骗监控、检测和分层的用户鉴权的多个级别的系统和方法，包括：指印模块，用于识别已经向服务器请求连接的用户装置；鉴权模块，用于使得能够根据预定的选择标准来从多个登录图形用户界面中进行选择以呈现在所述用户装置上，其中，所述选择标准具有关于可用性和安全性的规则的形式；欺骗分析器和警告模块，用于根据对所述用户装置的使用历史的跟踪来分析和估计与所述用户装置相关联的风险；以及装置中央库，用于根据所述指印模块和跟踪信息的其他库来识别合法和欺骗的用户。本发明提供了各种架构的系统，用于实现本发明的方法以向一个或多个服务提供商提供鉴权服务。

[0032] 本发明的可用性和安全特征的一个示例由忘记了它们的登录 ID 或密码的用户提供。这样的用户通常从有限数量的用户装置访问系统，并且本发明识别从这样的装置进行这种类型的鉴权尝试的事实，并且所述事实可以用于向用户提供有帮助的界面。如果所述系统不知道所述装置，则这可以表示黑客正在试图闯入所述系统，并且可以用于提供安全性提高的鉴权界面。另外，这样的用户通常输入几乎但是不完全正确的其用户 / 密码信息。这可以被本发明识别，并且用于进一步引导用户鉴权。在优选实施例中，这些选择被由规则引擎处理的规则表示。

[0033] 本发明的可用性和安全性特征的另一个示例由用于区别用户行为的能力提供。如果访问发起自先前没有访问过服务提供商的用户装置（例如由在用户装置上存储的装置权标的不存在检测到这一点），则系统规则可以要求这个访问通过更高级别的鉴权或者质询。但是，用户可以是机智的用户，其从它们的用户装置例行地去除应用权标（几乎 15％的因特网用户）。而且，根据先前的访问，这个用户可以与用于指示来自不容易识别的装置的例行访问的行为模式相关联。因此，这个用户优选地不被质询或者进行更高级别的详细审查。相反，具有不根据过去的用户动作而调整鉴权处理的鉴权系统的系统总是质询这样的用户。因此，本发明向所有用户提供更好的用户体验，而不论它们是否机智。

[0034] 进一步详细而言，本发明的系统和方法验证每个用户的计算机和位置（“你所具有的”）以及用于确认身份的在站点上的动作使用模式（“你所充当的”）。这些验证被加在现有的企业的对登录 / 密码证书的要求上（“你所知道的”）。这向企业提供了反欺骗保护的若干强大的附加层。

[0035] 本发明包括安全 cookie、flash 对象和其他技术，用于从用户从其访问应用的那个装置识别和通过指印验证是否它是计算机、笔记本计算机、移动装置或者任何其他。这些用户装置因此变为附加的鉴权因素而不要求在用户行为上的任何改变。关于这些用户装置的信息被获取指印和存储到装置权标或者装置 ID 中用于一次使用。所述 ID 和权标被存储在用户装置上，并且被保存在数据库中以以后与从随后的用户装置访问检索的权标相比

较。如果用户试图重新使用它，则所述权标被无效。

[0036] 本发明还包括用户装置权标或者装置 ID，它们具有由本发明的方法随机产生的唯一的编号。这样的装置权标然后被分配到特定的用户装置，在所述特定的用户装置上被存储为永久数据（例如 cookie），并且也被存储使得本发明的鉴权服务可访问。由此，可以通过从用户装置检索装置权标和将所述唯一编号与所存储的信息相比较，在随后的访问时识别所述特定的用户装置。如果所述数据匹配，则识别了这个特定的装置。然后，通过本发明的方法建立新的唯一标识符编号，并且将其存储在用户装置上，以用于进一步的访问。

[0037] 本发明使得应用服务提供商能对每个在线登录和交易的风险进行评分，并且对于可能具有高风险或者可能的欺骗的交易在登录和在会话中实时地提高鉴权安全性。其评估每个交易的在会话之前、之后和之中的特性，以保证欺骗检测和交易完整性。所述方法然后向服务提供商提供分数、动作和警告。例如，如果交易具有高风险分数并且因此可能是欺骗的，则一个优选的动作是挂起所述交易，然后寻找辅助的鉴权或者辅助的质询。用户例如被请求给服务提供商人员打电话来确认被挂起的交易的有效性。另一种动作是拒绝交易。不同的动作对于不同的交易类型可能是适当的。在银行服务提供商的情况下，查看账户余额是可接受的，但是电汇 (wire transfer) 是不可接受的；或者在电子商务 /ASP 服务提供商的情况下，可以根据风险分数来限制敏感文件的下载。这些动作优选地通过在交易评估期间评估的规则调用。

[0038] 本发明的系统和方法包括下面的特征：装置、位置和用户行为（“工作流”）指印获取；通过对用户工作流的捕获和记录来进行的用户简档建立；实时的风险评分；实时的基于规则的欺骗警告和响应；警告；可疑活动的自动内部标记；可配置的带外终端用户可选的辅助鉴权（经由电子邮件、SMS、声纹等）；经由开放的 API 的第三方集成；对于共享的鉴权和欺骗服务基础设施的支持；用于察看单独的客户日志的情况管理工具；用于服务于所输入的客户关心的客户关心工具；用于实时欺骗和动作监控的仪表板；风险管理和趋势分析的报告；以及，系统和规则配置和维护的管理。所述方法和系统包括下面的组成部分和特征：规则引擎；风险分数提供 / 取证；实时的响应；装置、位置、工作流的专有指印获取；模型和规则；智能算法；以及，综合管理工具，诸如仪表板、报告和客户关心 (customer care)。

[0039] 通过下面的说明、所附的权利要求和附图，本发明的这些和其他实施例、特征、方面和优点将变得更好明白。

附图说明

[0040] 通过结合附图参见下面的详细说明，本发明的上述方面和伴随优点将变得更容易明白，其中：

[0041] 图 1 是图解用于输入用户鉴权信息的示例现有技术系统的图；

[0042] 图 2 图解了用于使得能够经由鼠标点击选择来输入鉴权信息的现有技术小键盘图形用户界面；

[0043] 图 3 图解了用于使得能够经由鼠标点击选择来输入鉴权信息的现有技术键盘图形用户界面；

[0044] 图 4A-4B 图解了用于描述本发明的系统和方法的指印获取方面的示例实施例的

流程图；

[0045] 图 5 图解了用于描述用以说明本发明的系统和方法的示例实施例的处理的流程图；

[0046] 图 6 图解了按照本发明的一个实施例的欺骗分析器和警告系统 (FAAS) 方面；

[0047] 图 7 图解了按照本发明的一个实施例的、用于使得能够根据选择标准选择多个登录图形用户界面之一的鉴权器的方框图；

[0048] 图 8 图解了按照本发明的一个实施例的图形轮式两因素鉴权界面，用于使得能够使用鼠标点击导航（以对齐字母数字和图形符号）来输入鉴权信息；

[0049] 图 9 图解了按照本发明的一个实施例的示例图形滑块鉴权界面，用于使得能够使用鼠标点击导航（以对齐字母数字和图形符号）来输入鉴权信息；

[0050] 图 10A 图解了按照本发明的一个实施例的可选择的更高安全性的小键盘图形鉴权界面，用于提供更高的安全性，其中包括在图 2 的界面内重新排序字母数字符号；

[0051] 图 10B 图解了按照本发明的一个实施例的可选择的更高安全性的小键盘图形鉴权界面，用于提供更高的安全性，其中包括单向在图 2 的界面内偏移小键盘；

[0052] 图 10C 图解了按照本发明的一个实施例的可选择的更高安全性的小键盘图形鉴权界面，用于提供更高的安全性，其中包括在另一个方向上在图 2 的界面内偏移小键盘；

[0053] 图 10D 图解了按照本发明的一个实施例的可选择的更高安全性的小键盘图形鉴权界面，用于提供更高的安全性，其中包括在图 2 的界面内的字母数字小键盘输入选项的扭曲；

[0054] 图 10E 图解了按照本发明的一个实施例的可选择的更高安全性的小键盘图形鉴权界面，用于提供更高的安全性，其中包括在图 2 的界面的一部分的重新排序以及加阴影；

[0055] 图 11 是图解按照本发明的一个实施例的示例装置中央库 (DCR) 系统和方法的流程图；

[0056] 图 12 是图解图 11 的加标记的装置模块 (FDM) 的一个实施例的方框图；

[0057] 图 13A 和 13C 图解了本发明的示例系统实现方式；

[0058] 图 13B 图解了本发明的示例方法结构实现方式；

[0059] 图 14 图解了本发明的优选功能配置；

[0060] 图 15A-15B 图解了例证策略集和要包括在所述例证策略集中的例证安全模型；

[0061] 图 16A-16C 图解了本发明的外部对象和模型的优选结构；

[0062] 图 17A-17D 图解了示例管理工具。

[0063] 在附图中使用附图标号或者名称来表示其中所示的特定部件、方面或者特征，附图标号对于多个指示其中所示的部件、方面或者特征的附图是公共的。

具体实施方式

[0064] 本发明一般地提供了与在线服务提供商的服务提供系统连接的系统和方法，并且在对它们的用户请求、特别是用户登录请求和交易序列（在此被称为用户的“工作流”）进行鉴权方面帮助它们。简而言之，本发明以由装置（鉴权请求发起自这个装置）的身份和关于请求用户的身份的可用信息这两者确定的方式对用户和登录请求进行鉴权（在此被称为“前鉴权”）。使用用户的交易历史对用户工作流序列进行鉴权（在此称为“后鉴权”）。

在两种应用中，可以在来自服务提供商的规则引导下进行精确的鉴权处理和判定。

[0065] 优选的系统配置

[0066] 现在说明这些系统和方法的优选实施例的一般结构和布置，随后更详细地说明分处理的优选实施例。在此仅仅使用标题以便清楚，并且没有任何意欲的限制。

[0067] 图 13A 图解了本发明的一个示例实施例，其涉及向在线服务提供商提供鉴权服务，所述在线服务提供商使各用户可以获得在线服务器应用。一般，所述服务器应用在服务提供商服务器上执行。所图解的实施例包括一个或多个服务提供商计算机系统，例如系统 1302 和 1304，和鉴权系统服务器系统 1306，它们通过网络 710 与一个或多个用户装置 720 互连，用户在所述用户装置处进入登录和随后的交易请求。系统服务器 1306 的结构一般是本领域公知的，并且包括 CPU、RAM 存储器、盘或者其他数据库存储器 1308、通信接口和可选的用户接口设备等。数据库 1308 存储在鉴权处理中使用的数据，诸如装置和用户历史。所述网络也可以一般具有在本领域中公知的结构，并且可以是专用内联网或者公共因特网等。用户装置（用户从其向服务器应用发出请求）可以是工作站类型的计算机、PC 类型的计算机、终端等。

[0068] 在许多优选实施例中（但是无限制），使用客户机 - 服务器类型的架构（或者更一般而言为分布式系统类型的架构）来实现本发明的鉴权处理。因此，提供用于特定的服务提供商的应用的鉴权服务的单独处理可以在服务提供商的计算机系统上执行或者被分布在其他附接到网络的计算机系统之间。优选的分布式架构包括一个或多个鉴权服务器，其至少具有装置中央库（“DCR”）服务。

[0069] DCR 接收、存储在线信息 1310 并使之可用，所述信息用于识别用户装置和与用户装置相关联的欺骗风险。这个信息可以包括分别具有较高的欺骗风险的和具有较低的欺骗风险的装置的黑名单和 / 或白名单。可以从参与实现本发明的服务提供商的鉴权经历或者从本发明的其他同时和相互通信的实现方式、从第三方数据源等收集这个信息。鉴权服务器也可以具有服务提供商应用。

[0070] 作为选用，鉴权服务器也可以具有本发明的实际鉴权处理，所述处理因此被配置为对来自在服务提供商计算机系统上远程执行的应用的请求进行响应的服务器处理。由此，在本发明的某些实施例中，鉴权服务器系统也提供“基于装置的鉴权服务”以及“DCR 服务”。服务提供商服务器系统（例如系统 1304）自身不需要运行所有（或者任何）鉴权处理，而是可以在鉴权服务器上访问它未具有的那些处理（或者所有的鉴权处理）。在其他实施例中，服务提供商系统可以执行所有的鉴权处理，因此仅仅需要访问所述鉴权服务器来获得选用的 DCR 服务。在图 13A 中，系统 1302 本身不执行前鉴权处理，而是执行“后鉴权服务”。

[0071] 在另一个优选实施例中，可以在防火墙机器（或者其他类型的网络网关机器）上执行鉴权服务，通常是前鉴权服务。在图 13A 中，防火墙 1305 主要执行服务提供商系统 1304 的前鉴权业务。如果用户被鉴权，则那个用户可以访问服务提供商应用，例如应用 A、B、C、D 等。在某些情况下，防火墙可以执行所有的前鉴权服务处理；但是，在大多数情况下，有益的是，防火墙作为鉴权服务器的鉴权服务的客户机。事实上，防火墙即使在服务器的帮助下执行全部的前鉴权处理也可能是不实用的，在这种情况下，它可以执行鉴权处理的子集（在此称为“基本鉴权服务”）。

[0072] 基本鉴权服务可以限于用户装置指印获取和基本机器数据（例如IP地址、操作系统、装置ID等）的确认。如下所述，用户的计算机具有包括机器的识别信息的cookie。这个cookie在登录时被防火墙查看以验证其与所述实体所了解的关于用户的信息相匹配。差别可以被识别和评分，以确定是否允许访问或者是否在允许访问之前应用辅助鉴权协议，诸如安全问题。这个实施例可适用于诸如组织、公司或者律师事务所之类的实体，用于鉴权其雇员、成员或者其他用户的远程登录，其中，这些雇员或者用户的数量为大约10,000或者更少。

[0073] 图13B图解了计算机实现的处理，它们合作来提供本发明的鉴权服务，主要是前鉴权服务。在所图解的优选实施例中，这些处理具有如图中的环绕的虚线中所示的结构，并且包括：指印处理400、欺骗分析和警告服务（“FAAS”）、鉴权器服务600和带有标记的装置模块（“FDM”）。通过重要的输入和输出数据类型来标注在处理之间的链接。

[0074] 当服务器应用或者服务提供商计算机系统接收到需要鉴权的用户请求1320时调用鉴权服务。在前鉴权的情况下，最普通的用户请求是访问应用或者系统的登录请求。由后鉴权服务通常处理的其他请求包括例如涉及大量货币的交易请求。可以直接地从通信子系统接收用户请求，或者，可以通过接口从服务提供商应用或者系统向鉴权处理转发所述用户请求。

[0075] 在优选实施例中，可以通过外部可以获得的应用编程接口（“API”）来调用鉴权服务。表1列出了示例API请求的选择。

[0076]

表1－API请求的示例

#	描述	动作	请求XML	响应XML
1	获得装置的指印的前鉴权请求	**FingerPrintRequest**	FingerPrintRequest.xml	FingerPrintResponse.xml
2	更新鉴权会话的鉴权状态	**UpdateAuthResult**	UpdateAuthResultRequest.xml	FingerPrintResponse.xml
3	处理所述规则	**ProcessRules**	ProcessRulesRequest	ProcessRulesResponse

[0077] 通常从服务提供商应用发送第一请求，以开始已经从其接收到用户请求的装置的鉴权。当服务提供商应用希望查看用于执行例如高价值交易的鉴权状态时可以发送第二请求。最后，第三示例请求可以提供规则，并且根据表征用户或者会话的当前鉴权信息来处理它们。

[0078] 指印处理400是使用用于描述用户请求的输入数据而调用的第一鉴权处理。指印处理然后收集识别信息，所述识别信息用于描述发起用户请求的装置，并且所述指印处理建立装置标识符（“装置ID”）。所述装置ID（以及作为选用的其他装置识别信息）被存储在用户装置上，从所述用户装置可以检索所述装置ID，并且所述装置ID形成要在随后的指

印获取期间使用的装置识别信息的一部分。

[0079] 接着，使用装置 ID（以及作为选用的其他装置和 / 或用户识别信息）来调用 FAAS 处理 600。这个处理评估其输入的识别信息，并且可以例如向服务提供商应用或者系统推荐所述请求应当被进一步处理或者从系统被阻挡（在此称为“动作”）。这个处理也可以提供风险警告和风险分数（在此称为“警告”和“分数”），用于描述输入请求的相对风险，以便服务提供商应用或者系统本身可以进行这样的鉴权判定。FAAS 评估优选地开始于检索与在输入的请求信息中明显的当前请求的特性相关联的取证信息 (forensic information)。信息源可以包括系统 DCR 服务（其存储鉴权系统的过去的鉴权结果）和第三方数据服务（其可以提供大范围的数据），所述第三方数据服务诸如用于提供当前请求的可能的地理源的地理位置数据服务。输入数据和检索的取证数据然后被基于规则的判定处理分析，以便确定输出动作、警告和分数。

[0080] 换句话说，装置 ID 通常可以被获得，因此是用于识别被授权的用户的主要项目。即使当识别了装置 ID 时，也可以要求用户在被允许访问之前提供另外的安全信息。可以使用其他的传统安全协议（即私人问题、从多选择问题选择个人信息等）或者甚至更高的安全级（即电话 IP 管理器、用于提供语音识别的呼叫等）。当用户预先知道不同的计算机将用于在特定时间的访问时，例如考虑到使用不同计算机的到新的地点的商务旅行，则这个信息可以被提供到实体及其 IP 管理器，以便那个特定用户和时段的规则可以被改变以便利对于系统及其应用的访问。

[0081] 如果要进一步处理一个请求，则进一步的示例动作是选择优选的图形（或者其他类型的）鉴权界面（“GUI”），用于对发出需要具体鉴权的请求的新到达的用户或者现有的用户进行鉴权。可以按照评估的风险分数和任何风险警告来确定鉴权界面选择标准。所述选择标准然后要求与欺骗风险相当的界面。而且，也可以向服务提供商系统或者应用提供所述风险信息，所述服务提供商系统或者应用然后执行例如更彻底的鉴权数据查看或者请求本发明的鉴权服务对用户或者请求进行重新鉴权。这可以涉及例如寻找对于细节鉴权问题的响应，或者获得生物统计学识别信息（例如指印、视网膜扫描等），或者获得声纹等。

[0082] 接着，鉴权器处理 700 被使用界面选择标准来调用，按照所述标准从用户界面数据库选择特定的用户鉴权界面，然后在发起的用户装置呈现所选择的界面，并且接收响应于界面呈现而输入的数据。所输入的数据然后被本发明的处理的服务提供商应用 1322 用作鉴权判定的一部分。服务器应用或者 FAAS 或者两者一起然后确定是否对当前的请求进行鉴权。

[0083] DCR 处理收集当前的请求鉴权处理的结果，并且将它们与发起用户装置的识别信息（例如装置 ID）相关联地存储在 DCR 数据库 110 中。这些被存储的处理结果优选地至少包括是否所述请求被验证为有效的并且 / 或者是否所述请求被发现是欺骗的。由此，DCR 数据库可以提供前一个请求鉴权处理的结果的历史记录以在当前的鉴权请求处理中引导 FAAS。DCR 数据库至少包括从当前的服务提供商获得的数据。优选的是，它也包括来自其他服务提供商的数据，以便可以共享装置风险信息，并且可以将鉴权处理的精度加倍。

[0084] FDM1200 执行当前的请求鉴权处理的结果的实际收集和组配 (assembly)。可以作为选择地用第三方数据作为对来自当前请求的数据的补充，所述第三方数据类似于已经由 FAAS 检索的数据和 / 或与评估当前请求相关联的、由 FAAS 检索的其他数据。FDM 处理可以

作为鉴权服务的一部分本地或者远程地执行，或者可以被实现为 DCR 服务的一部分。

[0085] 图 13C 图解了对于可以由防火墙或者路由器调用（在本地调用或者远程调用）的基本鉴权服务的一个示例实施例的计算机实现的处理。这个特定的实施例仅仅执行按照本发明对规则引擎处理 701 进行鉴权所需要的最小处理。当用户请求被例如防火墙接收时调用这个处理，并且这个处理接收用于描述所述请求的信息。在一种替代方式中，这个处理从用于描述用户交易的输入数据和自数据库 1809 检索的规则（由服务提供商提供或者是可以从鉴权系统获得的默认规则）来确定动作和分数。所述规则可以是前摄的或者反应的。例如，可以阻止访问，除非欺骗风险较低，或者可以允许访问，除非欺骗风险较高。在其他替代方式中，处理 701 也可以从 DCR 数据库和 / 或第三方来源检索数据并且依赖于所述数据。然后，提供动作、分数和 / 或警告以进一步由防火墙 1322 处理。

[0086] 换句话说，当系统发现提高的风险分数时，其根据所述风险分数来评估规则，并且可以执行动作、警告或者风险分数报告。表 2 提供了对于提高的风险分数的响应的优选类别。

[0087]

表 2 – 事件和风险评分引擎
确定和输出加权风险分数
可定制的门限
可定制的动作
可定制的警告

[0088] 一种示例动作是设置内部标记或者向审查列表添加，以便服务提供商可以随后跟踪。另一种示例动作是最好基于质询响应模型的在线或者带外辅助鉴权。例如，在线辅助鉴权可以要求用户对被发送到注册的电子邮件地址的电子邮件进行响应。带外鉴权可以包括各种生物统计，诸如声纹，其可以要求用户口头地对质询进行响应。

[0089] 本发明的方法检索关于请求发起自的装置、发出请求的用户和由那个用户请求的交易的信息。本发明的有效处理是有益的，特别是在同时服务于大量用户的商务应用中。因此，在许多优选实施例中，所收集的信息被存储用于以浓缩或者汇总的形式在线使用，并且用于以近乎完全或者完全细节离线使用。在线使用例如包括实时鉴权和鉴权更新。离线使用例如包括数据挖掘、规则精练等。

[0090] 一种优选的浓缩或者汇总的形式在此被称为指印。首先，数据类别的或者鉴权标准的可能值被划分为多个“箱”。然后，特定用户的所述类别或者标准指印是所收集的数据的表示（例如作为二进制权标），其仅仅指示哪些箱子具有数据，哪些没有。可以使用已知的技术来选用地压缩这种表示。由此，可以以几个二进制权标 (binary token) 来表示用户的鉴权和交易请求。

[0091] 例如，在典型的在线业务应用中，可以有 20 个唯一的预先识别的敏感交易序列（工作流）。每个工作流可以被特征化为例如 10 个箱子或者变量，并且每个变量具有例如 10 个赋值。因此，用户可以由固定数量的可能指印来表征，其中每个用户平均例如具有 10 个唯一的指印。

[0092] 优选的功能配置

[0093] 本发明的功能被配置来提供用于查看对于服务提供商应用（例如在线商店应用、在线银行应用等）作出的用户启动的请求的真实性和安全性的一致方法。所述方法接收请求本身或者用于描述和抽象当前请求的内容的信息的拷贝。所述输入信息被处理，并且所述方法输出风险分数、风险警告和动作（或者动作推荐）。风险分数和警告是当前请求错误、或者恶意或者欺骗等的可能风险的标记。更具体而言，风险分数输出是多个欺骗检测输入的乘积，所述多个欺骗检测输入被使用对于单独的服务提供商可定制的分析处理实时地加权和分析。欺骗检测输入描述用户、用户的装置、用户装置的位置、由用户输入的交易工作流、用户访问的历史模式和来自第三方数据来源的数据。这个信息被提供到服务提供商应用和系统（本发明的“使用者”）以用于它们的内部鉴权处理。本发明的方法也可以按照服务提供商指南或者规则推荐或者启动动作。这些动作一般涉及收集用于对正在被处理的请求进行鉴权的信息。

[0094] 一般，与用户请求相关联的可用的、与安全性有关的信息（“请求属性”）被划分为被称为标准的相关信息群组，以便每个标准优选地包含关于用户请求的几个数据。规则组（优选地是与标准相关的）然后评估所述标准，并且从每个标准的基于规则的评估的结果的组合和加权产生被输出的风险分数和动作。因为用户请求、特别是用户交易的相关组被本发明鉴权并且被服务提供商应用处理，因此可以获得或多或少的标准数据，并且标准具有不同的重要性。例如，在用户被鉴权和许可访问服务提供商应用之前，通常不能获得与工作流标准相关的数据（例如由用户进行的相关交易的序列）。另一方面，当用户请求交易时，与初始鉴权相关的标准通常不太重要。这些时段分别被称为“前鉴权”时段和“后鉴权”时段。

[0095] 优选的前鉴权标准包括位置信息和装置信息，优选的后鉴权标准包括用户信息和工作流信息。表 2 提供了与这些标准的每个相关的示例数据。

[0096]

表 3 – 请求属性的示例		
前鉴权	位置信息	城市、州、国家信息和置信度因子 连接类型 连接速度 IP 地址、路由类型和跳跃次数 因特网服务提供商标记 自治系统编号 运营商名称 顶级域 次级域 注册组织 匿名代理的列表 主机名和路由器
	装置信息	安全 cookie Flash cookie 数字签名的装置 装置和显示特性： 操作系统特性 浏览器特性
后鉴权	用户信息	用户标识 有效或者无效用户 鉴权状态
	交易信息	关键字值对： 多重支持 可以使用正则表达式来限定关键字 可以在多个范围内定义多个值 所访问的页面 在页面上花费的时间 交易序列

[0097] 图 14 图解了包括表 2 的请求属性和标准的示例功能配置。所述标准的请求属性被浓缩为指印：位置指印、装置指印、工作流指印和历史数据指印。所述指印然后被处理以

产生动作、警告和分数。可能的动作包括主要鉴权，其是对用户进行识别和鉴权的处理。主要鉴权主要基于位置和装置指印，并且可以包括在用户装置处提供安全登录屏幕。另一个动作是辅助鉴权，如果需要鉴权确认或者进一步鉴权，则辅助鉴权可以在会话期间被调用。其可以包括使用例如电子邮件和声纹等。

[0098] 这个附图也图解了可以在评估处理中包括第三方数据。第三方数据可以被并入各种指印中。例如。第三方数据可以包括在用户装置上的防火墙或者反病毒软件的存在与否，并且 / 或者也包括这样的软件的维护状态。第三方数据也可以包括 IP 智能、风险数据、历史数据（来自数据仓库）和欺骗网络数据等。而且，用于描述在位置、装置或者用户级的已知风险的第三方描述特性可以被第三方数据仓库接收，并且被并入到各种指印中，主要是工作流指印和历史数据指印。而且，第三方评估工具可以被集成到评估指印的分析和评分处理中或者作为所述分析和评分处理的补充。

[0099] 位置信息和装置信息是重要标准，特别是在前鉴权时段中。位置信息表征请求发起自的装置的位置。从装置的 IP 地址和将装置链接到因特网的位置的分层来估计位置是最容易的。装置信息表征发起装置本身，诸如其硬件和软件组件。表 3 表示可以通过使用浏览器所包含的处理从装置提取的装置软件和硬件特性的更详细的目录。

[0100]

表 4 – 示例硬件和软件特性

装置信息		HTTP 首标	Flash 共享对象
操作系统	操作系统	X	X
	版本	X	
	补丁	X	
浏览器	浏览器	X	
	版本	X	

[0101]

	补丁级	X	
	Http 协议版本	X	
硬件	屏幕 DPI		X
	具有麦克风		X
	具有打印机支持		X
	具有音频卡		X
	屏幕分辨率		X
	屏幕颜色		X
软件	具有音频编码器		X
	支持视频		X
	具有 MP3 编码器		X
	可以播放音频流		X
	可以播放视频流		X
	具有视频编码器		X
位置	位置	X	
	语言	X	X
	语言变化形式	X	

[0102] 装置信息的另一个重要分量（当可以获得时）是可以从先前被用作用户装置的装置获得的安全权标，例如安全cookie。当从装置接收到请求时，至少可用位置和装置信息可以被汇总、浓缩或者获取指印，并且被存储回装置上来作为安全权标。如果另一个请求随后发起自这个装置，则可以检索所述安全权标，并且将其内容与当前收集的位置和装置信息相比较。可以对任何不匹配进行加权以形成用于风险分析的分数。不论是否发生不匹配，新的安全权标都被从当前检索的信息产生，并且被存储回所述装置上。

[0103] 这样的安全权标也有益地包括由本发明的方法产生的唯一标识符。将在所检索的权标中的唯一标识符与预期的或者已知的唯一标识符相比较，这提供了关于分数所基于的进一步的信息。而且，如果不能从用户装置获得位置或者装置信息，则唯一标识符特别有益。因此，所述唯一权标可以是唯一的识别装置信息。

[0104] 优选的后鉴权信息包括用户信息和交易（或者工作流）信息。用户信息包括用户标识和通过用户鉴权处理的用户的进展。交易信息包括从被请求的交易提取的信息和交易的次序和定时。优选的是，通过查找关键字表达然后提取其值（可能仅仅是值的范围）和与关键字相关联的其他信息，从交易请求提取信息。交易的次序和定时与所访问的网页的次序和定时被封装到工作流指印（其是用户历史使用模式的汇总）中。

[0105] 图 14 也指示通过由规则引擎驱动的欺骗分析来实时地处理和评分如上所述被封

装到指印中的标准数据。为了同时向多个服务提供商和服务提供商应用提供鉴权服务，优选的是，将分析和限定这样的处理的规则编组为功能上相关联的模块，它们被看作实质上通过规则引擎可交换。因此，通过使得一般的规则引擎（或者一般的规则引擎的一些实例）在模块之间转换，鉴权服务可以被提供到各种服务提供商。每个服务提供商可以通过提供更多的这种模块来限定其本身的鉴权服务。

[0106] 因此，优选的是，以在此被称为策略的群组来实现分析。表 5 图解了对于大多数系统有用的优选的策略。其他系统可以具有所需要的一些不同的策略。

[0107]

[0108]

表 5 – 策略

安全策略	异常检测 误用检测 侵入检测 预定黑客模型 可定制的模型
业务策略	会话中交易监控 业务限定的交易规则 关键字值驱动的逻辑 可定制的模型 事件、时间和值模式识别
工作流策略	历史交易 行为分析 时间分析 自动分类 用户简档 预定的可定制的风险模型

[0109] 可以在前鉴权期间（例如当用户正在被鉴权时）或者在后鉴权期间（例如当用户正在发出交易请求时）实施策略。规则引擎自动确定要基于请求的环境来运行什么模型。可以配置不同组的模型来支持不同的交易类型，例如账单支付、货币转帐、密码改变、电子邮件改变等。因为以 XML 来定义和撰写所述模型，因此在初始集成后，在服务提供商应用中不需要任何代码改变。可以使用网络接口或者通过替换 XML 定义文件来修改所有的模型。而且，可以在本发明的方法的操作期间无缝地增加新的模型。模型完全是可移动的，因此它们可以从一个仿真环境迁移到一个测试和生产环境。另外，可以对于例外（例如“用户不在

用户列表中”或者“装置不是银行工作台”）配置策略；可以基于例如时段或者一次性例外来暂时忽略策略。

[0110] 简而言之，安全策略可使用前后鉴权，并且通常设法识别已知的黑客动作。可以使用从跨产业的最佳实践开发的标准来识别这些动作。当交易会话正在进行时，业务策略主要是适用的后鉴权。这些策略一般表示由特定的服务提供商建立的，用于减轻交易风险的标准。工作流策略主要是适用的后鉴权，并且将过去的交易会话活动的指印与当前会话的指印相比较，以便检测可能指示欺骗的意外模式。

[0111] 图 15A 图解了实现诸如表 4 的策略的策略的功能配置。按照在适用于鉴权阶段的所有策略中的分析来分析（最好是同时）每个进入的请求。然后将策略和它们的分析的确定组合为对于各种门限值加权的加权风险分数，以便产生适当的动作、警告和分数。可以对于每个服务提供商定制所述加权、门限值、动作和警告。

[0112] 现在，以安全策略开始，更详细地说明优选的安全、业务、工作流和第三方策略。安全策略可以被广泛地应用到大多数服务提供商和服务提供商应用上，并且在前后鉴权期间都被使用。它们可以例如在用户登录期间和在用户交易处理期间被应用。安全模块一般从装置和位置标准评估多个数据项，它们被评估来获得安全分数。图 15B 图解了这样的数据项的示例集。例如，在不可能地短的持续时间中提交看起来从多个机器或者多个城市或者多个位置发起的请求的用户已经被发现可能是黑客。因此，这些和类似的数据项是优选的安全模型的一部分。

[0113] 所述安全策略包含涉及基于与用户、装置和位置信息相关联的风险模式的判定的模型。所述安全模型基于已知的风险条件和可能的冒险行为，并且被分类为下面的模型。表 6A 和 6B 提供了说明性的安全模型。

[0114]

表 6A – 受限的模型

基于位置的规则	从受限国家（例如 OFAC（外国资产管制处）国家）的登录 从受限的 IP 地址的登录 从受限的匿名器和代理的登录
基于用户的规则	从受限的用户列表的登录 用户的多个连续故障
基于装置的规则	从受限装置的登录 来自装置的多个连续故障 使用盗用的 cookie 的装置 第一次使用装置的用户

[0115]

图 6B – 黑客模型	
基于位置的规则	在给定的时间段内从不同地理位置（城市、州或者国家）的用户登录 在给定的时间段内从给定的 IP 地址的多次登录
基于用户的规则	在给定的时间段内从不同地理位置（城市、州或者国家）的用户登录
基于装置的规则	在给定的时间段内从不同装置的用户登录 在给定的时间段内来自给定装置的多次故障 在给定的时间段内从给定装置的多次登录 在给定的时间段内从不同的地理位置使用的同一装置

[0116] 服务提供商可以发现与用户请求相关联的特定条件要求必须防止这个用户的访问。受限模型收集与确定必须防止特定访问相关的数据项和因素。或者，服务提供商可以发现特定的用户动作模式表示这个用户是黑客或者恶意的。黑客模型因此收集相关的数据项和因素。

[0117] 表 7 提供了与安全策略相关联的数据项的另一个示例。

[0118]

表 7 – 采样安全策略数据项

定时的用户城市	用户：来自城市	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
定时的用户国家	用户：来自国家	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
定时的用户装置	用户：来自装置	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
定时的用户 IP	用户：来自 IP	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
定时的用户的 IP 类 C 地址	用户：IP 子网	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
定时的用户状态	用户：来自州	rule.type.enum.user	查看是否是用户最后的登录尝试	{过去的秒数}
数字 cookie 不匹配	用户：cookie 不匹配	rule.type.enum.device	查看是否是用户发送的 cookie	
装置的非尝试状态	装置：使用错误状态登录	rule.type.enum.device	除给定状态之外的最多登录尝试	{鉴权状态} {最后尝试数目}
装置的尝试状态	装置：使用真实状态登录	rule.type.enum.device	具有给定状态的最多登录尝试	{鉴权状态} {最后尝试数目}
装置的组中	装置：在组中	rule.type.enum.device	如果装置在其中	{组 ID}
定时的装置用户数量	装置：最多用户	rule.type.enum.device	对于过去的 x 使用这个装置的最多用户	{过去的秒数}{最大数量
完全获取指印	装置：被获取指印	rule.type.enum.device	查看是否从所有可识别所述用户	
位置的 IP 组中	位置：来自 IP	rule.type.enum.location	如果 IP 在 IP 范围中	{组 ID}
位置的范围组中	位置：来自 IP 范围	rule.type.enum.location	如果 IP 在 IP 范围中	{组 ID}
使用同一位置的多个用户	位置：最多用户	rule.type.enum.location	使用当前 IP 的用户的最大数量	{过去的秒数}{最大数量
不在 IP 组中	位置：不在 IP 中	rule.type.enum.location	如果 IP 不在 IP 中	{列表 ID}
不在范围组中	位置：不在 IP 中	rule.type.enum.location	如果 IP 不在 IP 中	{列表 ID}
在城市中的 IP	位置：在城市中	rule.type.enum.location	如果 IP 在给定的当中	{组 ID}
在国家中的 IP	位置：在国家中	rule.type.enum.location	如果 IP 在给定的当中	{组 ID}
在州中的 IP	位置：在州中	rule.type.enum.location	如果 IP 在给定的当中	{组 ID}
不在城市中的 IP	位置：不在城市中	rule.type.enum.location	如果 IP 不在给定的当中	{组 ID}
不在国家中的 IP	位置：不在	rule.type.enum.location	如果 IP 不在给定的当中	{组 ID}
不在州中的 IP	位置：不在州中	rule.type.enum.location	如果 IP 不在给定的当中	{组 ID}

[0119] 这些数据项是从位置、装置和用户标准组配的（如在列 2 中所示）。用户类型数据项一般测试是否特定用户的动作显示了可能的恶意意图。装置类型数据项一般测试特定的装置是否被以显示所述特定装置已经被用户以可能恶意的意图访问的方式来已经使用和 / 或正在使用。例如，如果一个装置是过去发出过被拒绝的登录请求的装置或者被无法识别的可疑用户访问过的装置，则所述装置可疑。这些数据项也包括装置 ID 或者指印，如果可以从所述装置获得的话。位置类型数据项一般测试装置或者用户与 IP 地址的关联性。例如，如果用户或者装置的请求发起自多个 IP 地址或者新的 IP 地址等，则所述用户或者装置是可疑的。

[0120] 评估规则与诸如图 15B 或者表 7 的模型的安全模型相关联，所述评估规则在一个优选实施例中提供了反映当前请求是安全问题的可能性的分数。表 8 和 9 以判定表的形式提供了示例的安全评估。所图解的判定处理被分层地排列（或者嵌套），其中，如果发现特定条件，则表 8 调用另外的查看，诸如表 9 的查看。

[0121]

表 8 – 主要装置判定表

关键字：X＝丢失；M＝存在并且不匹配；*＝存在并且匹配

数据项	安全 cookie	Flash cookie	Flash 数据	浏览器特性	操作系统特性	分数
	*	*	*	*	*	0
	X	*	*	*	*	模式查看
	M	*	*	*	*	辅助查看
	X/M	X	*	*	*	模式查看
	X/M	M	*	*	*	辅助查看
	X/M	X/M	X	*	*	模式查看
	X/M	X/M	M	*	*	辅助查看
	X/M	X/M	X/M	M	*	辅助查看
	X/M	X/M	X/M	X/M	M	10

[0122] 如果对于当前的用户请求，所有的被评估数据项都存在并且匹配，则这个表返回分数“0”（指示低的欺骗可能性的分数）。如果不存在数据项或者如果所有的数据项不匹配，则返回分数“10”（指示高的欺骗可能性的分数）。如果一些数据项存在并且匹配而其他数据项不存在或者不匹配，则这个表调用另外的查看。如果不存在被本发明预先存储在装置上的被检索的数据权标（例如安全 cookie、Flash cookie 或者 Flash 数据），则执行进一步的模式查看。所述模式查看检查位置和装置标准的模式的细节，并且分配适当的分

数。如果在数据权标中包括的数据与当前的位置和装置标准不匹配，则执行另外的辅助查看。

[0123] 辅助查看检查在被检索的数据权标中包括的数据如何不匹配与当前的用户请求相关联的标准的细节。表 9 是实现这样的辅助查看的示例判定表。

[0124]

表 9－辅助装置判定表

安全 Cookie 不匹配						
关键字	T＝真	F=伪	X＝丢失			
先 前 的 cookie（同一装置）	真					
浏览器特性	操作系统	ASN	ISP	IP	位置	分数
T	T	T	T	T	T	0
F	T	T	T	T	T	5
X	T	T	T	T	T	5
T	F	T	T	T	T	10
T	X	T	T	T	T	0
T	T	F	T	T	T	10
T	T	X	T	T	T	0
T	T	T	F	T	T	5
T	T	T	X	T	T	0
T	T	T	T	F	T	5
T	T	T	T	X	T	0
T	T	T	T	T	F	5
T	T	T	T	T	X	0
F	F	F	F	F	F	10
X	X	X	X	X	X	10

[0125] 在这个表中，ASN 是“自治系统编号”的缩写；ISP 是“因特网服务提供商”的缩写；IP 代表 IP 地址（这些全部是在通信领域中公知的）。消息发起地的优选的指示来自组合所述消息的 ASN、ISP 和 IP（与例如仅仅 IP 地址相反）。如果作为作为安全 cookie 不匹配

的结果而要求辅助查看，则收集所指示的数据项，并且从所述表确定分数，将所述分数返回到主判定表以调用特定的辅助查看。可以由不同的主判定表在不同的时间调用单个辅助查看。

[0126] 业务策略一般包括对于独立的会话中交易的参数评估欺骗或者恶意意图的可能性的规则（被称为“交易规则”）。因此，业务策略一般在后鉴权期间被应用到，一般是域(field)相关的或者服务提供商和服务提供商应用的业务相关的。例如，在银行应用中，特定的交易规则可以涉及特定的银行交易，诸如账单支付、款项划拨等。交易模型可以与安全规则相结合地被使用，例如不允许（或者向用户质询）来自国际 IP 地址的货币转帐请求。业务策略可以由在特定域中的不同服务提供商共享，或者可以对于特定的服务提供商建立和定制。

[0127] 例如，特定的银行服务提供商可能已经确定特定的交易数据表示应当限制或者拒绝交易。表 10 提供了评估条件的示例规则，所述条件可以表示应当限制、质询或者拒绝交易。

[0128]

表 10 – 受限的业务策略模型规则
货币转帐请求大于特定的美元量
去往和来自特定的可疑骗子或者国际账户的货币转帐请求
由从另一个国家登录的用户进行的特定美元数量的货币转帐请求
向非商人账户的账单支付大于特定的美元数量
来自未注册的装置/位置或者频繁使用的欺骗装置/位置的交易。这可以触发客户服务请求或者质询问题或者带外的电话鉴权

[0129] 工作流策略包含评估指示预期的动作模式的相关交易（例如由特定用户请求的交易）的组或者序列的模型。这些规则优选地基于给定类别的典型用户的期望或者基于描述特定用户的历史。相反，在工作流策略中的规则可以指示意外动作，所述意外动作可能指示恶意意图。例如，如果用户例行地请求在特定范围内的账户划拨，则远在本范围之外的划拨可以表示风险。或者，如果用户例行地进行大于预期平均的数量的货币转帐，则在所述部分范围内的未来的划拨不一定指示风险，并且可以对于所述用户有益地放松适当的规则。

[0130] 表 11 提供了规则的示例，所述规则表示所请求的交易是欺骗性的或者恶意的，并且应当被限制、质询或者拒绝。

[0131]

表 11 – 受限的工作流模型规则
由用户执行的超过平均数量的交易。这可以基于每日、每周、每月、每季度和每年
除了一天的正常时间之外，用户进行他的/她的交易
除了一周的正常时间或者一月的正常周之外，用户进行他的/她的交易
交易类型和美元数量的不规则模式

[0132] 另一种类型的策略和模型适用于其中来自第三方数据库的数据对于评估风险有用的情况。例如，相关的规则可以根据来自黑名单列出的 IP 地址的第三方数据库的输入来阻止或者限制登录或者交易。另外，相关的模型可以基于从外部数据库获得的欺骗模式或者模型。本发明的实施例维护对评估交易有用的数据库，并提供用于产生和模拟欺骗行为的模式的方法。

[0133] 上面已经描述了标准、策略和模型的结构。在运行中，对于在提供鉴权服务的过程期间变得已知的特定的装置、位置、用户、请求、服务提供商等建立和填充这些数据和规则类的特定实例。这些在此一般被称为“外部对象”。为了帮助更容易地定制对单独的服务提供商的鉴权服务，所建立的实例被编组在一起，并且被（尽可能地）评估为群组成员。所述群组对应于特定的标准项，并且链接到包含用于评估动作的规则的兼容模型。

[0134] 图 16A-16C 图解了用于将外部对象群组和特定的外部对象链接到指定评估和动作规则的模型的一个优选模型。模型是配置规则的集合。模型包含任何数量的规则。图 16A 图解了可能的（例如在过去被识别的）装置、位置、用户和工作流（优选的是工作流指印）每个被分配到这些对象的特定的各自群组。这些可能的外部对象的群组也被链接到将相关评估规则和策略编组的模型，例如强调所选择的数据项的判定表。不同的服务提供商然后可以从所链接的模型中选择要用于评估它们的请求的不同的模型。而且，不同的服务提供商可以提供用于链接到外部对象组的它们自己的模型（或者用于它们的建立的方向）。

[0135] 图 16B 图解了可能对于在特定会话中提交的用户交易建立的特定外部对象表示的示例。所图解的会话表示被特定用户在特定装置在特定位置提交的特定工作流。所述特定用户、装置、位置和工作流是这些相应的外部对象的所图解的群组的实例。这些群组被链接到包含评估规则的评估模型。优选的是，所述装置和位置群组被链接到一个或多个安全模型群组，而用户和工作流群组被链接到一个或多个业务模型和 / 或工作流模型。所图解的业务模型包含所指示的评估规则，其可能按照情况而引起所指示的动作或者警告。作为选用并且为了说明书的经济性，模型可以被编组为策略集，所述策略集通常包含每个类型的一个模型。然后，外部对象可以被链接到策略集而不是单独的模型。

[0136] 策略集保存用于评估总的风险分数的所有策略、模型和规则实例。可以配置、测试和存储多个策略集，但是在优选实施例中，实际上一次仅可以使用一个策略集。每个策略集一般包含四种策略，例如安全策略、业务策略、工作流策略和第三方策略，其中每个策略类型表示基于策略类型的模型。

[0137] 图 16C 图解了通过这种结构单个请求的处理。限定进入的请求的数据被用来更新在与这个请求相关联的策略集中的模型。这些数据更新可以使得触发风险 / 规则引擎。所

述风险 / 规则引擎可以然后输出所要求的动作、警告或者分数。

[0138] 更详细而言，所述群组、模型和规则可以按照业务需要被定制，以如果交易的分数大于特定的风险门限值则变得被激活。表 12 提供了一些示例的规则类型。

[0139]

表 12 – 临时允许/中止规则
在每个用户基础上
单个或者多个规则
基于时间或者计数

[0140] 而且，可以嵌套模型以保证风险分数的更高程度的精度。所嵌套的模型是用于在由系统输出的原始结果不确定的情况下进一步量化所述风险分数的辅助模型。仅仅当从主要模型返回特定的回答序列时，才运行被嵌套的模型。因此，被嵌套的模型减少了假的肯定和否定，并且用于保证风险分数的整体精度。如果服务提供商不希望分配用于特定标准和数据组合的风险分数或者嵌套的模型，则向每个属性附加默认的加权。这进一步改善了定制要求。

[0141] 显然，这个分层结构良好地适合于允许容易的定制，服务提供商仅仅需要指定它们的鉴权服务的一般目标，而在系统群组中隐藏特定细节。同样显然，这个模型适合于通过面向对象的编程技术来实现。所述系统规则引擎指导收集标准数据、建立外部对象和处理规则。

[0142] 所述规则引擎（图 14）在使用模型和策略及其数据元素之前分析它们。在鉴权服务期间，所述规则引擎当识别与先前分析的服务提供商模型相关的先前分析的数据元素时触发模型处理。交易数据流用来识别可能影响模型的元素。在触发后，所述模型执行和提供风险分数和动作和警告（如果要求的话）。新的或者被改变的参数和数据被保持以便当下次识别新的数据或者下次触发模型时测试它们。例如，如果新的数据在旧数据的特定范围内，则可能不需要触发相关联的模型。

[0143] 表 13 提供了规则引擎的一种优选的架构。

[0144]

表 13 – 规则引擎架构
专家核心
界面
语义框架
XML/Native/XLS 适配器

[0145] 在优选实施例中，所述规则引擎提供了通告已知的格式化语言和协定来构造的外部接口。在专家核心中包含的方法被设计来允许服务提供商准确地识别可能的欺骗和恶意意图。

[0146] 更详细而言，下面是核心方法的示例。一种示例方法被称为“在门限上的时间”。

这种方法在每个交易将变量的值与预先定义的门限值相比较，并且报告是否对于太多的交易所述值已经在范围之外。因此，不是每次通过门限值时触发模型，而是使用近来的历史数据来选出持续存在的问题。因此，在门限上的时间消除了不必要的警告和动作。另一种示例方法被称为“与通常的偏离”。这种方法不将当前的动作与固定的门限值相比较，而是使用历史数据来建立特定日期、时间、用户、装置、工作流等的正常值。然后，其评估是否当前的动作偏离在类似情况下通常的动作。

[0147] 另一种示例方法被称为“事件状态”。这种方法保存存储过去的警告和动作的外部对象的状态。然后，故障规则产生关于第一次故障的单个警告。随后的故障将不产生另外的警告，直到已经从第一警告过去了所选择的间隔。如果规则随后成功，则将清除所述警告。另一种示例方法被称为“事件率”。这种方法仅仅在已经在所选择的时间间隔的一部分中发生了太多次数的所选择事件后产生警告。例如，如果在一个小时中发生了超过 3 次的登录故障，则产生警告或者提醒，用于指示侵入者可能正在尝试访问系统。但是，在预定的时段期间的随后的登录故障将不产生另外的警告，少于三次的登录故障也不产生另外的警告。另一种示例方法被称为“在门限上的事件时间”。这种方法当所接收的陷阱 (trap) 率在超过门限率达一段时间时产生警告。例如，网络链路频繁地通断，因此如果每个链路周期都产生警告，则产生混乱。但是，如果网络链路在例如一个小时中已经例如故障了例如 10 分钟或者更久，则可用性可能被影响，并且产生警告。

[0148] 优选的软件配置

[0149] 现在更详细地说明已经如上简述的本发明的方法和系统的单独组件 :指印处理 (参见图 4A)，然后是 FAAS 处理 (参见图 5 和 6)，然后是鉴权器处理 (参见图 7-10)，然后是 DCR 服务器 (参见图 11)，最后是 FDM 处理 (参见图 12)。优选的是，使用与其他数据项 (诸如浏览器特性、装置硬件配置 (例如使用 Flash 调用所需要的)、网络特性等) 组合的安全 cookie、Flash cookie 和类似的数据权标来识别用户装置。通过可配置的一组嵌套的规则 (其识别装置，并且为了精确也查看来自这个装置的历史登录，包括处理其中 cookie 被禁止的例外情况、不同步的 cookie，并且也可能识别欺骗地盗用的 cookie) 来评估标识数据的装置。

[0150] 图 4A-B 是图解本发明的系统和方法的装置指印处理 400 的示例实施例的流程图。图 4A 提供了装置指印获取的更一般的视图，而图 4B 是图 4A 的精练，提供了装置指印获取的一个优选实施例的更详细的视图。本说明将主要参见图 4A，在图 4B 中的类似步骤因此容易显然。在步骤 402 中，在服务提供商服务器处从例如用户装置 720(图 13A) 接收对于其上驻留的数据的请求。所述指印获取处理被调用，并且描述所述请求的信息被传送。用户装置可以是像在图 13A 中那样的个人计算机 720、蜂窝电话、个人数字助理 (PDA)、自动柜员机 (ATM) 或者能够访问服务器的其他适当装置。优选的是，所述服务提供商服务器是可以从用户装置经由因特网、或者其他公共网络或者专用网络访问的万维网服务器。

[0151] 在步骤 404，捕获用户装置的装置身份信息。这个信息可以被已经在用户装置上驻留的客户端程序捕获。对于因特网应用，所述客户端程序通常是万维网浏览器。或者，可以向用户装置下载软件模块，并且执行所述软件模块以收集识别信息。对于因特网应用，所述软件模块可以是插件、脚本或者由万维网浏览器下载和被执行的小应用程序 (例如 Javaapplet)。所收集的身份信息被选择来尽可能唯一地识别用户装置。优选的是，可以在

访问服务器应用的那些用户装置内唯一地识别所述装置。如果能够获得的信息不足以用于唯一地识别，则尽可能窄地例如通过在可能的用户装置之间大幅度不同的特定属性的值来识别用户装置。身份信息可以被指印获取处理本身产生的数据增加，所述数据例如是唯一的比特串，诸如大随机数。装置身份（以及由指印获取处理产生的身份信息）信息中的一些或者全部被存储在被称为“装置 ID”的数据权标中，这个部分的附件 A 提供了在装置指印获取的特定优选实施例中有用的数据元素和评估规则的特定示例。

[0152] 一般，所捕获的装置识别信息包括下述内容。第一类型的装置识别信息是已经预先存储在用户装置上的安全的永久的数据权标。安全永久数据一般包括如下的数据元素，所述数据元素被加密、签名或者以其他方式防止修改，并且所述数据元素保持驻留在用户装置上，即使当其不访问服务提供商应用时也是如此。这个数据可能已经预先被服务提供商服务器应用存储在用户装置上，在这种情况下，所述数据经常标识访问服务提供商的用户。这个数据也可能已经通过本发明的指印获取处理在这个装置的先前识别过程期间存储，在这种情况下，它最好包括“装置 ID”。

[0153] 虽然可以使用允许远程应用在用户装置上存储和检索永久数据的任何技术，但是优选的是，使用已知和广泛可获得的技术。一种这样的技术被称为“安全 cookie”。标准的 cookie 是由万维网服务器向万维网浏览器发送的数据群组，以存储到在主机上的文件。所述数据群组可以在被请求时，例如每当浏览器向服务器作出附加请求时，被检索和发回服务器。安全 cookie 表示已经防止修改或者窜改的标准 cookie。

[0154] 另一种这样的技术被称为“flash cookie”。来自 Macromedia 的、一般被识别为商品名称“Flash”的图形软件应用和 / 或插件当前驻留在许多用户装置上。这个软件可以建立本地共享的对象，其被称为“flashcookie”，用于与由万维网浏览器存储的标准“cookie”类似地在用户装置上本地维护永久数据。flash cookie 可以被本地存储在 flash 插件用户装置上，可被更新，并具有不像标准 cookie 那样容易从用户装置去除的优点。

[0155] 第二种装置识别信息是用户装置和 / 或用户装置的网络连接的硬件特性。许多类型的硬件特性可以被收集来用于装置识别目的，包括 :IP 地址、适配器 MAC 地址、本地时间和 / 或时区、网络连接速度（诸如下载和 / 或上载时间）、微处理器类型和 / 或处理和 / 或序号等。在本部分的附件 B 中描述了用于这样的信息的收集的软件。

[0156] 在步骤 406 中，将所捕获的装置身份信息 (ID) （包括任何先前存储的装置 ID) 与先前已经由 FAAS 处理存储在数据库中的、被称为“装置 / 简档历史”（参见在图 6 中的 610，其中，所述装置 / 简档历史被称为“简档历史”）的身份信息相比较。所述装置历史 / 简档数据库包括记录，所述记录关联于并且描述先前识别和 / 或标识的装置。如果可以在测试 408 确定所捕获的装置信息对应于预先对于装置存储的信息，则新的识别信息在步骤 412 更新所述装置的装置历史记录。一种测试是匹配预先由指印产生、并且被存储在用户装置上和装置历史中的唯一比特串。如果在测试 408 期间没有发现在装置历史数据库中的对应记录，则在步骤 410 使用新的身份信息来建立新的记录。

[0157] 最后，在步骤 414，对于所述装置建立新的装置 ID 权标，并且在步骤 416，将所述新的装置 ID 权标发送到用户装置和存储在其上，例如存储为标准 cookie 或者 flash cookie。如果在用户装置上未发现装置 ID，则从所收集的识别信息建立新的装置 ID 权标。如果发现了装置 ID，则可以例如使用新的唯一比特串、新的时间戳等将其更新。在步骤 418，处理继

续。

[0158] 本发明的一个特征涉及在每次登录时替换用户机器上的 cookie。这进一步提供了安全性，以便即使用户的机器信息不适当地被第三方获取（甚至包括在前一个 cookie 中包含的用户机器信息），鉴权系统也可以识别所述用户未被授权，并且拒绝对于所述系统的访问。当然，由不同计算机的访问对于某些用户经常发生，并且可以提供辅助安全协议以允许访问授权用户。另外，如果允许来自在不同计算机上的用户的访问，则当用户试图访问在系统中的应用或者其他文件时可以通过实现了更高的风险安全的软件来识别所述访问。cookie 和装置权标一般也被存储来用于与当以后检索时的权标相比较。因此，不能欺骗地重新使用被盗用的指印、权标或者装置 ID。

[0159] 参见图 5 和图 6 说明由所述指印处理调用的欺骗分析器和警告系统 (FAAS) 处理，图 5 图解了这个处理的示例流程图，图 6 图解了这个处理的一种示例实现方式。一般，FAAS 的功能是“表示”用户和服务提供商的指令，所述指令是关于如何最佳地根据与发出访问请求的装置相关联的风险信息、并且可选地根据所述请求的特性，来执行鉴权。在优选实施例中，用户和服务提供商的指令由规则表示。FAAS 的规则引擎分量根据可用的欺骗风险信息来评估访问请求，以便确定鉴权界面选择标准。在替代实施例中，可以使用其他技术来评估访问请求，并且确定界面选择标准，例如，所述规则和规则引擎可以被替换为统计分析技术、神经网络技术等。例如参见 Duda 等，Pattern Classification（模式分类），Wiley-Interscience，第二版，2000 年。

[0160] 转向图 6，针对 FAAS600 的输入、输出、内部数据结构和处理分量而图解和说明 FAAS600。大多数外部输入被数据源处理模块 606 处理。这个模块接收外部数据和格式，并且 / 或者准备它以由规则引擎 604 使用。一种外部输入是由指印获取处理 500 刚刚收集的、关于当前的访问请求发起自的装置的装置识别信息。这个所收集的信息优选地包括（并且 / 或者被封装在）装置 ID，并且也可以包括 IP 地址、安全和 flash cookie、CPU 类型等。这个识别信息用于交叉参考装置 / 简档历史数据库 610，以便确定是否当前装置已经预先访问了所述服务提供商系统。如果如此，则其中存储的并且与当前装置相关联的信息（诸如风险信息）被检索和输入到数据源处理模块。所述装置 / 简档数据库被使用当前的识别信息更新。当不能唯一地识别装置时，这个信息表示包括当前装置的一组类似装置。

[0161] 从服务提供商系统到数据源处理模块的另一种外部输入是基于交易的输入 620。基于交易的输入 620 包括关于由用户装置正在请求的特定交易的输入，诸如购买数量、转帐数量、所请求的转帐类型，服务提供商或者用户可以希望通过在规则定义模块 608 中存储规则而特殊地处理它们。例如，在超过某一数量的购买请求被发送到服务器之前，服务提供商可能希望接收警告和 / 或调用更高安全性的鉴权界面。

[0162] 到数据源处理模块的另一个外部输入来自被标记的 (flagged) 装置中央库 (DCR)618。所述 DCR 是从服务提供商得出（并且优选的是也从其他服务提供商得出）的历史欺骗风险信息的数据库。从所述指印获取和 FAAS 处理得出所述信息。

[0163] 数据源处理模块也优选地从外部第三方数据提供商接收数据。这些来源可以包括地理位置服务 612、黑名单服务 614、白名单服务 616 等。地理位置服务 612 提供对应于用户装置 IP 地址的近似地理经度和纬度。按照 IP 地址的地理位置是通过将用户的 IP 地址与其他近处的服务器和路由器的已知位置相比较而确定对应于用户的地理经度和纬度的

技术，所述地理位置服务向其用户提供另一种武器，用于防止因特网欺骗。第三方黑名单服务 614 通常提供列表，该列表包含可疑的欺骗用户的 IP 地址，诸如与可疑的或者已知的欺骗动作相关联的地址。第三方白名单服务 616 通常提供具有合法、即不与欺骗相关联的历史的 IP 地址的列表。

[0164] 优选的是，FAAS 处理由规则引擎 604 执行。这个规则引擎可以如在本领域中已知的那样构造以使用预定的一组规则来确定鉴权界面选择标准。数据源处理模块耦接到规则引擎以便使得外部数据容易形成。规则定义模块 608 提供所存储的规则和动作。规则被存储在规则定义模块的分量 622 中；并且与规则相关联的动作被存储在存储器 624 中。规则可以由服务提供商提供和存储，以便可以针对服务提供商的要求来定制鉴权动作。服务提供商服务应用 1322 也可以选用地具有到规则引擎的直接链路，以便规则引擎向服务提供商应用请求附加的鉴权指南。

[0165] 一种示例动作是指定特定的鉴权界面选择。例如，规则可以指定：当从用户装置接收到传送在特定门限值之上的数量的货币的请求并且所述装置驻留在由地理位置信息确定的已知发生了大于正常数量的欺骗动作的位置，则要采取的动作是向用户提供预定的更高安全性的用户界面以便更安全地防止可能的欺骗交易。

[0166] 规则引擎按照所存储的规则来评估其输入数据（和输入指南（如果有的话）），并且按照所存储的动作来确定界面选择标准。所述界面选择标准指定应当在当前的用户装置向用户显示的鉴权界面的类型，以便对当前的访问请求进行鉴权。在一些实施例中，这些标准可以指定要显示的特定界面，或者在其他实施例中可以指定界面特性，诸如安全级别。所述界面选择标准被输出到鉴权器 700，该鉴权器选择和向用户显示所述鉴权界面。用户然后输入所请求的鉴权信息和 / 或执行所请求的鉴权动作（如果有的话）。被称为“用户鉴权信息”的这个被输入的信息被返回到 FAAS 和 / 或服务提供商应用以及规则引擎。规则引擎或者服务提供商应用或者两者一起评估所述用户鉴权信息以确定是否用户被鉴权。作为选用，可以确定鉴权程度。如果鉴权程度不足，则服务提供商应用可以然后请求 FAAS 执行进一步的鉴权。

[0167] 图 5 图解了一种示例的 FAAS 流程图。FAAS 处理当其接收到由指印获取处理从用户装置捕获的装置识别数据（诸如装置 ID）时被调用。身份和风险信息然后被规则引擎在 504 评估，以确定是否要向发出用户请求的当前装置提供预定 / 预先选择的用户界面。如果如此，则鉴权器功能 700 在 508 被调用以按照界面选择标准产生用户界面（优选地是图形界面），然后在 510 向所述装置提供所述界面。

[0168] 规则引擎然后评估所返回的用户鉴权信息以在 512 进一步确定是否需要其他形式的鉴权或者验证。按照由服务提供商指定的规则来在 514 执行附加鉴权（如果需要的话）。例如，可选步骤 514 可以是其中服务提供商是银行或者其他金融机构的情况，所述银行或者其他金融机构寻找用于特定交易的更安全的鉴权界面。

[0169] 接着，规则引擎和 / 或服务提供商系统或者应用根据所接收的鉴权信息（诸如由用户输入的用户名和密码）来确定是否将用户鉴权为有效。如果用户有效，则处理在 520 对于在服务提供商万维网服务器处的服务提供商应用 1322 继续。如果用户无效，则用户被引导到错误消息页面 518。通常，服务提供商然后阻止用户访问万维网服务器，并且终止会话连接。或者，服务提供商可以向用户提供附加机会以提供有效用户鉴权信息。

[0170] 应当明白，服务提供商可能不向用户提供机会来使用用户输入界面来输入用于验证的鉴权信息。例如，如果基于所述 ID 信息来将用户装置识别为引起很大的欺骗风险，则本发明的系统和方法使得服务提供商能够经由规则要求向服务提供商发送欺骗警告。所述服务提供商可以然后通过在使得能够经由用户界面输入用户的鉴权信息之前中止用户到服务器的连接而响应。用于初始用户界面显示的选择标准可以由服务提供商预先确定。

[0171] 也应当明白，用户或者服务提供商可以例如根据被请求的交易，在有效的已经鉴权的会话的过程期间请求进一步的鉴权。例如，银行或者其他金融机构可能希望在超过特定数量的交易被发送到服务器之前在会话期间调用更高安全性的鉴权界面。本发明的系统和方法可以被调用来提供这样的鉴权。

[0172] 用户界面管理

[0173] 图 7 是鉴权器 700 的方框图。所述鉴权器根据由 FAAS 依赖于输入数据和规则确定的界面选择标准 730 经由网络 710 向用户装置 720 提供所选择的登录界面。所述选择标准可以包括多个可用性和安全性因素。例如，服务提供商或者所述服务提供商的用户 / 订户可以对于被感觉具有提高的欺骗风险的特定类型的交易请求提高了安全性的登录界面。这可以反映在对于服务提供商、对于特定用户或者对于特定的交易类型特定的规则中。

[0174] 本发明可以通过下述方式来处理可用性问题：通过提供范围从基本的普通用户界面到最安全的用户界面（其间有多个界面）的可选择的多层图形登录用户界面。例如，对于常规的交易，可以向正在使用不呈现已知的欺骗风险的装置的长期用户 / 客户呈现更用户友好的界面。在后一种情况下，可以对于那个用户建立规则，并且将所述规则包括为在图 6 中的定义模块 608 的一部分。而且，可以允许特定用户增加规则以定制他们的鉴权界面。

[0175] 更详细而言，界面选择标准 730 被在鉴权器 700 中的界面选择器 / 显示器 702 接收。界面模块 706 和数据库 704 耦接到界面选择器 / 显示器 702。数据库 704 包括多个图形用户界面 (GUI)，其被示出为“GUI1”到“GUI N”。所述 GUI 中被选择的一个 GUI 被界面选择器 / 显示器 702 根据界面选择标准 730 发送到界面模块 706。界面模块 706 经由网络 710 向用户装置 720 发送所选择的 GUI。作为选用，所述界面选择标准可以指定：以特定的方式来修改所选择的 GUI。所输入的用户鉴权信息被返回到 FAAS，并且 / 或者被返回到服务提供商。

[0176] 数据库 704 可以包括用户界面，诸如在图 1 中所示的界面 18 和在图 2、3、8 和 9 中所示的界面及其变化形式，例如如图 10A-10E 中所示，图 10A-10E 图解了基于在图 2 中的小键盘用户界面的多个更高安全性的界面。所述多个用户界面被示出为具有两个鉴权因素，即用户 ID 或者用户名和密码，但应当明白本发明不限于两个因素；可在本发明范围内包括另外的因素。所示的每个 GUI 被使用适当的软件（例如 MACROMEDIAFlash，Java 等）发送到用户装置。在优选实施例中，Flash 软件被用于所述 GUI。

[0177] 在图 8 和图 9 中的 GUI 通过下述方式提供提高的安全性：通过使得用户能够使用在线图像（其是以实际图像形式以及以数据输出形式不可识别的）输入和提交密码或者其他敏感信息。在下述文件中具有用于提供所述“不可识别的”在线图像的方法的进一步的细节：待决的美国专利申请序号 11/169,564，其在 2005 年 6 月 29 日被提交，并且通过引用被整体并入在此。图 8 图解了图形轮式双因素鉴权界面，用于使得能够使用用于对齐字母数字和图形符号的鼠标点击导航来进行鉴权信息输入。图 9 图解了示例图形滑块鉴权界面，

用于使得能够使用用于对齐字母数字和图形符号的鼠标点击导航来进行鉴权信息输入。应当明白，在图 8 和 9 中所示的符号和字母数字是示例性的，即，可以使用其他的图形符号和图像来实践本发明。

[0178] 在图 8 中的轮式 GUI800 可以被鉴权器产生和存储，并且包括至少两个同心的轮 802 和 804，用于在数据输入点加密。为了输入用户名字段 810 或者密码字段 812 的下一个元素（或者符号或者字符），用户经由在“右箭头”按钮 806（用于逆时针旋转）上和在“左箭头按钮”808（用于顺时针旋转）上的导航鼠标点击，将内轮 802 上的参考点引导到在外轮 804 上的期望元素。用户选择参考点，并且仅仅用户知道所述参考点，使得对于外方而言图像不可解释和 / 或不可识别，所述外方包括各种间谍软件和“在肩上的”间谍。

[0179] 每次用户点击“下一个”按钮以输入图像符号时，向服务器发送用于描述内轮 802 已经从其先前的方位移动的位移的数据，所述数据优选地作为度或者弧度或者类似的角度测量单位。所述“输入”按钮优选地用于指定用户名字段 810 或者密码字段 812 的元素要被输入。所示的所述按钮标识符仅仅是示例性的，可以使用其他的按钮标识符来用于本发明。或者，优选地仅用一个按钮取代其中用户名或者密码具有固定长度的系统的“下一个”和“输入”按钮。优选的是，被输入的元素不被显示在用户名字段 810 或者密码字段 812 中，来帮助防止“在肩上的”间谍查看所述字段信息。例如，星号可以选用地被显示在所述字段中以表示每个元素的输入。

[0180] 以度（或者弧度或者类似的角度测量单位）测量的内轮 802 的位移随后被发送到服务器，并且被服务器解码。鉴权器知道真实的鉴权信息和图像细节，因此通过解码所述位移信息以便确定 / 解码用户输入，导出所选择的标记，以对所述会话进行鉴权。位移坐标是会话相关的，并一旦会话结束则不可用。

[0181] 图 9 图解了按照本发明的另一个实施例的示例图形滑块鉴权界面 900。所述滑块界面 900（也被称为标尺）包括用户名输入字段 902、密码输入字段 904 和用于移动滑块的可选择的箭头按钮 906A 和 906B。或者，键盘箭头按键也可以用于移动滑块。滑块 900 包括：下行 908，其具有符号（或者字符）序列，即具有王牌符号 912，即“♠”，其对于这个示例在字母“B”之下；以及固定的上行 910，其具有要输入的元素（字符）的序列。下行 908 在操作中根据在“左箭头”按钮 906A 和“右箭头”按钮 906B 上的用户导航点击而可滑动地位移。滑块 900 的可移动的下行 908 的位移被相对于固定上行 910 测量，并且一旦用户使用“输入”按钮 914 表示输入则被发送到服务器并且被服务器解码。因此，滑块 900 的位移信息向鉴权器的发送的一般原理类似于轮 800 的一般原理。

[0182] “复位”按钮 916 优选地被提供来使得用户能够重新开始输入用户名或者密码。优选地在用于显示字段输入的状态的两行的右侧提供块图标 918，即指示已经输入了多少用户名或者密码的元素。优选的是，所输入的元素不被显示在用户名字段 802 或者密码字段 904 中来帮助防止“在肩上的”间谍查看所述字段信息。或者，可以在输入项输入部分中显示星号以表示每个元素的输入。

[0183] 图 2 图解了已知的数字小键盘形式的图形用户界面。所述小键盘图像优选地是在数据库 704 中的可选择的 GUI 之一。图 10A-E 图解了对于标准小键盘界面的更高安全性的用户界面修改，其提供了 5 个附加的可选择的层，它们比标准的小键盘界面更安全。这些界面可以被鉴权器存储，或者可以被鉴权器例如从图 2 的界面产生。

[0184] 图 10A 图解了第一可选择的更高安全性小键盘图形鉴权界面，其将在图 2 中的界面中的字母数字符号重新排序。小键盘 1010 包含在图 2 的数字小键盘 20 中的数字的重新排序的显示的一个示例。所述重新排序通过对于在小键盘图像上的数字具有不同的 x-y 坐标，提供了针对鼠标点击 x-y 坐标记录器的附加的安全性。

[0185] 图 10B 图解了第二可选择更高安全性小键盘图形鉴权界面 1020，其在一个方向上偏移在图 2 中的界面的小键盘 20。在图 10B 中的小键盘界面 1020 通过偏移小键盘而提供了针对鼠标点击和 x-y 坐标 23 记录器和屏幕捕获器的附加的安全性。在图 10B 中的重新排序的缺点是具有光学字符识别 (OCR) 的复杂屏幕捕获器可以解密例如在小键盘中的每个数字位于相对的 x-y 坐标中的位置，并且将此交叉引用到鼠标点击的 x-y 坐标，以便确定输入的数字序列。

[0186] 图 10C 图解了第三可选择的更高安全性小键盘图形鉴权界面 1030，其在另一个方向上偏移在图 2 中的界面的小键盘 20。

[0187] 图 10D 图解了第四可选择的安全小键盘图形鉴权界面，其使得在图 2 中的界面中的字母数字小键盘输入选项扭曲。在下述申请中更详细地说明了扭曲图形用户界面的方法：待审的美国专利申请序号 11/169,564，其在 2005 年 6 月 29 日被提交，并且通过引用被整体并入在此。小键盘 1040 通过扭曲图像和数字字符而提供了相对于屏幕捕获 /OCR 和鼠标点击 x-y 记录器的附加保护。所述扭曲使得用户能够容易地识别在图像中的数字，同时防止屏幕捕获器 /OCR 和 x-y 坐标记录器将鼠标点击链接到特定的数字。

[0188] 图 10E 图解了第五可选择的更高安全性小键盘图形鉴权界面 1050，其对图 2 中的界面的一部分重新排序和加阴影。在小键盘界面 1050 中的有斑点的阴影提供了相对于依赖于在图形图像上的校验和以便解密在数字小键盘的每个数字的 x-y 位置，以便盗用用户名或者密码的间谍软件的保护。与在图 10A 中的图像相比较，有斑点的阴影改变了所得到的校验和，并且通过与像在图 10B 中那样的小键盘数字的重新排序耦合，提供了增强的安全性。

[0189] 应当明白，图 10D 的扭曲方法以及在图 10A-E 中的其他修改方法也可以被应用到其他的图形用户界面，例如像在上述的美国专利申请中那样扭曲键盘（诸如图 3 的键盘 30）。相反，本发明不限于上述的扭曲技术，而是包括用于增强安全的在本领域中公知的其他扭曲技术。

[0190] 装置中央库服务

[0191] 图 11 是图解用于针对多个服务提供商（例如服务提供商 1-N）存储和报告历史装置风险信息的示例装置中央库 (DCR) 系统 1100 的方框图。所述 DCR 系统包括 DCR 服务器应用，其驻留于万维网服务器 110（其优选地与服务提供商的万维网服务器分离）上并在其上执行。DCR 万维网服务器 1110 被使得一个或多个服务提供商用户（其被图解为在万维网服务器 1120、1122 到 1130 上的服务提供商 1-N）可以通过适当的公共网络或者专用网络（诸如公共因特网）来访问，并且根据由本发明的指印获取模块收集的装置识别信息（当它们被服务提供商应用调用时）提供预定的欺骗风险信息。所述服务提供商应用通过由在每个服务提供商处执行的被标记的装置模块 (FDM) 1200 提供的设施来与 DCR 服务器应用通信。

[0192] 图 12 是图解 FDM 实施例的方框图。被标记的装置模块 1200 包括标记规则引擎

1210、规则定义模块 1220、共享列表处理模块 1240 和服务提供商鉴权（有效 / 无效）数据模块 1230。首先转向被标记的规则引擎，其输入包括由本发明的方法和系统产生的信息以及从外部第三方数据提供者检索的信息。由本发明的系统和方法产生的输入信息的重要分量包括服务提供商鉴权信息 1230。这个信息描述了当前用户访问请求的鉴权结果，诸如是否当前访问请求有效和 / 或欺骗。

[0193] 由指印获取模块 400 从用户装置 1260 收集的装置识别信息也被输入。这个识别信息类似于被输入到 FAAS600 和存储在数据库 610 中的身份信息 500。因此，所述身份信息优选地包括 IP 地址、标准 cookie、flashcookie 和其他识别信息。所附加的附件描述了获得其他识别信息（用于 CPU 类型 / 处理速度和连接速度识别）的方法。其他已知的标识符也可以用于识别用户装置，并且可以依赖于安全性级别和在过去从用户装置可访问的信息。

[0194] 来自第三方数据提供者 1250 的信息也被输入。这个输入一般在内容上类似于到 FAAS600 的第三方输入。像 FAAS 那样，这些包括第三方地理位置数据 612、第三方黑名单数据 614 和第三方白名单数据 616。

[0195] 所述组合的输入信息以及当前装置识别信息被发送到 DCR，其中，所述信息被用于更新历史风险数据库。所述组合输入信息还被标志规则引擎 1210（应用规则定义 1220）评估，以便维护基于历史信息的、并且可选地以一个或多个特定用户装置为目标的标识装置和它们的相关联的欺骗风险的列表。由所述标记规则引擎引导，共享的列表处理 1240 建立、更新和以其他方式维护黑名单 1242 和白名单 1244。所述列表是基于装置的，用于标识装置和由每个装置引起的可能欺骗风险。

[0196] 这个信息被使得可以被 FAAS 获得（在图 6 中的输入 618）。这个信息也被输出到在图 11 中的 DCR 服务器 1110。DCR 然后可以使得订购的服务提供商经由网络可获得共享列表（以及可选用地可获得另外的风险信息），或者可以被公布以便使得第三方卖方可以获得所述列表以使用。

[0197] 虽然已经说明了本发明的具体实施例，各种修改、改变、替代结构和等同内容也被涵盖在本发明的范围内。因此要在说明性而不是限定性的意义上看待说明书和附图。但是，显然在不脱离在权利要求中给出的本发明的更宽的精神和范围的情况下，可以对于本发明进行增加、减少、删除和其他修改和改变。

[0198] 管理工具

[0199] 本发明也包括管理工具，其帮助系统操作员和服务提供商提供和监控鉴权服务。

[0200] 图 17A 图解了一种这样的工具，其被称为“仪表板”(dashboard)。所述仪表板具有图形界面，其允许通过用户、装置和来源国的定制查看，并且提供向在进展中的可能欺骗动作中的一瞥的可视性。仪表盘提供了受保护站点的健康状况的实时视图。其包含一组默认的监控器，所述监控器可以以任何形式被组合以跟踪特定的一组动作。可以对于每个用户定制以仅仅显示所感兴趣的监控器。监控器是用于汇集实时跟踪器信息的机制。监控器可以对从无效用户到来自特定国家的登录尝试的任何东西进行计数。一些默认监控器包括：通过状态的尝试登录；新的装置；第一次登录；警告计数；以及位置计数（用于特定位置或者位置群组）。在已经定义了监控器后，它们可以通过指定监控器和表格类型而用于仪表板视图中。

[0201] 警告浏览器给出了在鉴权和交易查看点触发的警告的详细列表。其通过提供利用用户、装置、地理位置和警告组织的相关影响分析来识别哪个用户 / 交易处于欺骗行为的风险下。本发明也可以经由电子邮件、寻呼机、通过将警报转发到网络管理系统或者通过调用任何用户指定的动作，自动向适当的人员或者甚至终端用户通知所述警告 / 交易。

[0202] 图 17B 图解了可以定制仪表板以仅仅显示用于趋势目的的特定警告，而不是所有可能的警告。例如，机构可能要仅仅监控具有红色警告的所有电汇，而不是所有的其他交易。

[0203] 另一种工具是可定制的报告，其提供详细的风险管理和分析信息。报告可以提供包括地理位置、装置和用户的历史信息。图 17C 图解了示例报告。可在一个或多个报告中提供由本发明的方法访问的大多数数据。

[0204] 另一种管理工具提供了情况管理，其使得服务提供商能够查看每个单独客户的服务日志，并且调查采取动作或者触发警告的原因。图 17D 图解了客户关心工具的示例屏幕。

[0205] 例如，服务提供商人员可以查看登录或者交易被阻止的原因，查看具有警告状态的严重性标记以帮助自动调整 (escalation)，完成诸如发出对于客户的暂时允许，或者解除装置的注册（如果适当的话）等的动作。可以按照角色和公司规程来定制和管理在客户的欺骗分析器部件中的能力和观看权利。

[0206] 附件 A

[0207] 在装置指印获取中有用的数据项

[0208]

使用情况	征兆
新装置使用情况	

安全和 flash cookie 都被使能。	安全和 flash cookie 都丢失。flash 请求成功地通过。
安全和 flash cookie 都被禁止。	
安全 cookie 被使能，flash 被禁止。	安全和 flash cookie 都丢失。而且，flash 请求未成功地通过。
安全 cookie 被禁止，flash 被使能。	安全和 flash cookie 都丢失。但是，flash 请求成功地通过。
通常模式	
安全和 flash cookie 都被使能。	安全和 flash cookie 都到来。
安全和 flash cookie 都被禁止。	安全和 flash cookie 都丢失。而且，flash 请求未成功地通过。
安全 cookie 被使能，flash 被禁止。	仅仅安全 cookie 成功地通过。
安全 cookie 被禁止，flash 被使能。	仅仅 flash cookie 成功地通过。
例外	
浏览器升级	浏览器字符不匹配
装置升级	flash 数据不匹配
浏览器和装置升级	浏览器和 flash 数据都不匹配
使用不同的浏览器。安全 cookie 丢失	安全 cookie 丢失。浏览器特性不匹配。flash cookie 匹配。flash 数据是匹配（除了浏览器之外）
用户不同的浏览器。cookie 和浏览器特性不匹配。	安全 cookie 不匹配。浏览器特性不匹配。flash cookie 匹配。flash 数据是匹配（除了浏览器之外）
安全 cookie 不同步，flash 同步	安全 cookie 不匹配，但是属于同一

[0209]

	装置
flash cookie 不同步，并且安全 cookie 同步	flash cookie 不匹配，但是属于同一装置
安全 cookie 和 flash 都不同步	两种 cookie 不匹配，但是它们属于同一装置
其他模式	这些使用通常和例外模式的组合之一
用户使用多个浏览器，并且 flash 被使能。	
用户使用多个浏览器，cookie 被禁止，并且 flash 被使能。	
使用同一装置的家庭	
使用同一账户的家庭	
使用同一装置、同一账户、不同浏览器的家庭	
使用同一装置、不同账户、不同浏览器的家庭	
带着它们的笔记本计算机旅行很多的用户	
旅行很多并且使用公用电话亭 (kiosk) 的用户	
旅行很多并且使用笔记本计算机或者公用电话亭的用户	
旅行很多但是总是使用无线卡的用户	
旅行并且使用它们的笔记本计算机上的公共 wifi 的用户	
欺骗情况	
盗用的安全 cookie 和盗用的 flash	

[0210]

cookie。具有盗用的浏览器特性和 flash 数据 盗用的安全 cookie,没有 flash 请求。具有盗用的浏览器特性 盗用的安全 cookie,没有 flash 请求。浏览器特性不匹配 cookie 被禁止,盗用的 flash cookie。具有盗用的浏览器特性和盗用的 flash 数据 cookie 被禁止,盗用的 flash cookie。具有不匹配的浏览器特性和盗用的 flash 数据 cookie 被禁止,盗用的 flash cookie。具有不匹配的浏览器特性和不匹配的 flash 数据 cookie 被禁止,并且 flash 请求不具有 flash cookie。并且盗用的浏览器特性和盗用的 cookie 数据。 安全 cookie 不匹配,并且属于另一个装置	

[0211] 在装置和位置指印获取中有用的规则条件

[0212]

安全/flash cookie特性	描述
cookie丢失	服务器未接收到cookie
cookie不匹配	cookie被接收,但是不匹配在文件中存储的cookie
cookie无效	所接收的cookie无效
cookie属于同一装置	cookie与在文件中存储的cookie不匹配,但是属于来自前一次登录的同一装置
cookie属于另一个装置	cookie与在文件中存储的cookie不匹配,并且属于在系统中的另一个装置
对于同一浏览器特性,cookie最后n次丢失	用户以同一浏览器特性在最后n次登录,但是没有cookie
flash禁止	flash请求未到来
浏览器特性	描述
浏览器首标匹配百分比	整体匹配百分比
已知的浏览器首标属性匹配百分比	浏览器首标的所选择的已知属性的加权匹配百分比
操作系统被升级	是否操作系统被升级
浏览器被升级	是否浏览器被升级
flash数据	描述
flash数据匹配百分比	整体匹配百分比
flash被升级了吗	已经升级了flash版本了吗
操作系统被升级	操作系统被升级了吗?这是经由flash调用被识别的
装置的位置查看	描述
在装置简档中的IP	是否存在这个装置的从这个IP的先前的成功登录

[0213]

在装置简档中的 IP 子网	是否存在这个装置的从这个 IP 子网的先前的成功登录
在装置简档中的 ISP	是否存在这个装置的从这个 ISP 的先前的成功登录
在装置简档中的地理位置	是否存在这个装置的从这个 ASN 的先前的成功登录
在装置简档中的时区	是否存在这个装置从这个时区的先前的成功登录
位置识别规则条件	
地理位置置信度因子	由给定的 IP 地址的位置卖方返回的置信度因子
先前位置之间的距离	在两个位置之间的距离
是使用匿名器的登录吗?	用户正在使用匿名代理连接到服务器
IP 在 IP 列表中吗?	查看是否 IP 存在于给定的 IP 列表中。可以从外部数据库或者从另一个来源输入所述列表
是来自地理位置列表的登录吗?	查看是否在给定的位置列表中存在用户登录的位置
来自 ISP 列表的 ISP 吗?	查看是否这个 IP 所属的 ISP 在给定的 ISP 列表中
在用户简档中的位置?	是否存在这个用户从这个位置的先前的成功登录

[0214] 附件 B

[0215] CPU 检测

[0216] 第一方法使用在所列出的 CPU 之间的细微差别来在它们之间区别。在括号中示出了检测方法：

[0217] Intel i386SX(具有 POPAD bug)

[0218] Intel i386DX(没有 FPU)

[0219] Intel i486SX(在标记寄存器中存在 AC 比特)

[0220] Intel i486DX(在标记寄存器中具有 ID 比特,签订 CPUID 指令支持)

[0221] Intel Pentium(没有 FPU)

[0222] Cyrix Cx486S(Cyrix CPU 不:在划分后改变未定义的标记)

[0223] Cyrix Cx486DX(没有 FPU)

[0224] NexGen Nx586(NexGen CPU 不在划分后改变 0 标记)

[0225] NexGen Nx586FP

[0226] AMD Am386SX(40MHz)

[0227] AMD Am386DX(50 和 66MHz)

[0228] Intel i486DX2(100 和 120MHz)

[0229] AMD Am484DX4(66 和 80MHz)

[0230] Cyrix Cx486DX2(100MHz)

[0231] Cyrix Cx486DX4(所有版本,80 到 150MHz)

[0232] Cyrix 6x86(从 166MHz 起的所有版本)

[0233] Cyrix Ijx86MX(40MHz)

[0234] 仅仅对于支持 CPUID 指令的那些 CPU 执行第三种方法。即,在 1983 年引入的第一 Intel Pentium 后制造的大体上所有的 CPU。而且,从 1994 年起的所有的新的 486 支持这个指令。但是,安装了 Cyrix 5x86、Cyrix 6x86 和 NexGen CPU 的母板通常在 BIOS 中使得这个指令被禁止;为了获得正确的检测,需要通过软件来将其使能。这个 CPUID 指令返回关于 CPU 类型的足够的信息以使得所有的新的 CPU 可以容易地被识别。下面的 CPU 通过这个方法被识别:

[0235] Intel i486DX

[0236] Intel i486SX

[0237] Intel i486DX2

[0238] Intel i486SL

[0239] Intel i486SX2

[0240] Intel i486DX4

[0241] Intel i486DX4 OverDrive

[0242] Intel Pentium

[0243] Intel Pentium OverDrive

[0244] Intel Pentium MMX

[0245] Intel Pentium MMX OverDrive

[0246] Intel Pentium Pro

[0247] Intel Pentium II OverDrive

[0248] Intel PenIium II

[0249] flltel Pentium II Xeon

[0250] Intel Pentium II PE(mobile)

[0251] Intel Celeron

[0252] Intel Celeron A(Slot1)

[0253] Intel Celeron A(Socket370)

[0254] Intel Pentiun III

[0255] Intel Pentium III Xeon

[0256] Intel Pentium III E

[0257] Intel Pentium III E Xeon

[0258] UMC U5S

[0259] UMC U5D

[0260] UMC U486SX2

[0261] UMC U486DX2

[0262] AMD Am486DX2

[0263] AMD Arn486DX4

[0264] AMD Am5x86

[0265] AMD KS

[0266] AMD K6

[0267] AMD K6-2

[0268] AMD K6-III

[0269] AMD Athlon

[0270] Cyrix Media GX

[0271] Cyrix Media GXm

[0272] Cyrix 5x86

[0273] Cyrix 6x86

[0274] Cyrix 6x86MX

[0275] Cyrix M-II

[0276] Centaur/IDT Winchip

[0277] Centaur/IDT WinChip 2

[0278] Centaur/IDT WinChip 2A

[0279] Centaur/IDT WinChip 213

[0280] Centaur/IDT WinChip 3

[0281] Rise mP6

[0282] NexGen Nx586

[0283] NexGen NxS86FP

[0284] NexGen Nx686

[0285] 可以在几个级上执行 CPUID 指令。CPUID 指令的第一级返回卖方相关串：

[0286] " Genuinelntel- 由 Intel 处理器返回

[0287] " AuthenticAMD" - 由 AMD 处理器返回

[0288] " Cyrixlnstead' - 由 Cyrix 处理器返回

[0289] " NexGenDriven" - 由 NexGen 处理器返回

[0290] " CentaurHauls" - 由 Centaur/IDT 处理器返回

[0291] " RiseRiseRise" - 由 Rise 处理器返回

[0292] " UMC UMC UMC" - 由 UMC 处理器返回

[0293] CPUID 指令的第二级返回关于类型、家族、模型、指令改变（修订）和其他 CPU 特征的信息。

[0294] 这个应用可以包含小数据库，其向这个所检测信息加上短说明。此处是由 CPUID 返回的值的简短说明。

[0295] 类型具有这些值：

[0296] 0- 表示 TestCPU 正在使用在系统中的主要（或者唯一）的 CPU

[0297] 1- 表示安装了 OverDrive 处理器，即通过直接替换在旧母板上的 CPU 而进行的升级

[0298] 2- 表示在多处理器系统中的辅助 CPU

[0299] 家族几乎等同于代，并且表示 CPU “性能”类：

[0300] 4- 所有的 486、AMD 5x86、Cytrix 5x86

[0301] 5-Intel Pentium 和 Pentium MMX、AMD K5 和 K6、Cytrix 5x86、所有的 Centaur/IDT

[0302] Winchip, Rise mP6

[0303] 6-Intel Pentium Pro, Celeron, Pentium II 和 Pentium III, AMD Athlon,

[0304] Cyrix 6x86MX 和 M-I1

[0305] MODEL 是指定在家族中的模型的数量 :

[0306] 例如在家族 4 中 :

[0307] 0-i486DX

[0308] 3-i486DX2

[0309] 8-i486DX4

[0310] 例如在家族 5 中 :

[0311] 2-Pentium

[0312] 4-Pentium MMX

[0313] 例如在家族 6 中 :

[0314] 1-Pentium Pro

[0315] 5-Pentium II

[0316] 6-Celeron

[0317] 7-Pentium III

[0318] 注意, 所有这些 CPU 来自 Intel。其他制造商的 CPU 将不使用这个方案。

[0319] 指令改变 :这个数量按照在 CPU 设计中的小改变而递增。

[0320] BRAND(品牌) :来自 Intel 的新的字段, 用于区别它们的 CPU 的一些。已知值是 :

[0321] 0- 不被支持

[0322] 2-Intel Pentium IT1

[0323] 3-Intel Pentium III Xeon-

[0324] CPUID 指令的第三级仅仅被 Intel 第六代 CPU(来自 Pentium Pro) 支持, 并且返回关于由这些 16 进制值表示的高速缓冲存储器大小的信息 :

[0325] $06- 处理器具有用于指令的 8kB L1 高速缓冲存储器

[0326] $08- 处理器具有用于指令的 16kE3 L1 高速缓冲存储器

[0327] $0A- 处理器具有用于数据的 8kB L1 高速缓冲存储器

[0328] $0C- 处理器具有用于数据的 16KB L1 高速缓冲存储器

[0329] $40- 处理器没有 L2 高速缓冲存储器 (Celeron 检测方法)

[0330] $41- 处理器具有 128kB L2 高速缓冲存储器 (Celeron A)

[0331] $42- 处理器具有 256kB L2 高速缓冲存储器 (移动 Pentium II)

[0332] $43- 处理器具有 512kB L2 高速缓冲存储器 (Pentium II 和 ID)

[0333] $44- 处理器具有 1MB L2 高速缓冲存储器 (Xeon 版本)

[0334] $45- 处理器具有 2MB L2 高速缓冲存储器 (Xeon 版本)

[0335] $82- 处理器具有 256kB L2 高速缓冲存储器 (Pentium E)

[0336] $4x- 表示 4 路高速缓冲存储器 (全部)

[0337] $8x- 表示 8 路高速缓冲存储器 (Pentium III E)

[0338] CPUID 指令的第四级被从 Intel Pentium III 向上支持，并且返回处理器序号。

[0339] AMD、Cytrix 和 Centaur CPU 支持 :CPUID 的某些更高级，其可以用于检测特殊特征（例如 3Dnow ！ 技术）;它们的高速缓冲存储器大小或者串 (CPU 名称)，其是在芯片上被编码的。由这些 CPU 返回的串是 :

[0340] AMD-KS(tm) 处理器

[0341] AMD-K6tm w/ 多媒体扩展

[0342] AMD-K6(tm)3D 处理器

[0343] AMD-K6(tm)-2 处理器

[0344] AMD-K6(tm)3D+ 处理器

[0345] AMD-K6j(tm)-III 处理器

[0346] AMD-K7(tm) 处理器

[0347] IDT WinChip2

[0348] IDT WinChip2-3D AMD K5

[0349] AMD K6

[0350] AMD K6-2

[0351] AMD K6-2

[0352] AMD K6-III

[0353] AMD K6-III

[0354] AMD K7

[0355] Centaur/IDT C2

[0356] Centaur/IDT C2

[0357] 经由两种方法来确定 CPU 频率。第一种方法测量一些 CU 指令的执行时间，并且将这个时间与 CPU 类型的值的表格相比较。这些值是由所识别的 CPU 对于那个执行所需要的时钟周期的具体数量。我们的应用然后将相关值除以执行时间，得到 CPU 频率。

[0358] 本方法的一个缺点是 :如果未检测到正确的 CPU 类型，或者如果你具有所述表格中丢失的新的处理器，则不会精确地测量频率！

[0359] 经由第一种方法的频率检测 :

[0360] 执行所需要的时钟周期的数量（来自所述表格）/ 执行时间＝频率

[0361] 120000“滴答”/0.0012 秒＝ 100MHz

[0362] 第二种方法仅仅被应用到实现了时间戳计数器的 CPU。TSC 对处理器时钟周期进行计数。其在每个内部处理器时钟周期上递增，并且允许在 PC 上的最准确的定时方法。在处理器复位后，NB 这个计数器被复位到 0。其为 64 比特宽，如果一个处理器以 100MHz 运行，则所述计数器足够计数超过 5850 年。CPUID 指令用于查看实现的 TSC。所有的新的 CPU 将具有 TSC。Intel 从 Pentium 处理器向上、从 K5 开始的 AMD 和从 6x86MX 开始的 Cyrix 支持它。频率可以在理论上被测量到一个时钟周期的精度 ;实际上，时钟速率可以因为硬件因素而略微改变。即使如此，按照本发明的系统也可以将频率测量到 0.001MHz 的精度。

[0363] 经由第二种方法的频率检测 :

[0364] 1) 读取 TSC，并且将其写入 TI 变量中

[0365] 2) 等待精确的 1 秒（同时自动递增 TSC)

[0366] 3) 再次读取 TSC，并且将其写入 T2

[0367] 4) 从差 T2-T1 来计算以 Hz 计的频率

[0368] 性能等级评定 (P-Rating)

[0369] 一些 CPU 在频率之外具有 PR 后缀，用于表示性能等级评定。这个额外的标签来自处理器卖方 AMD、Cyrix 和 IBM，其希望显示它们的 CPU 具有更好的代码执行，并且比 Intel 的 Pentium 或者 Pentium II 处理器执行得更快（以给定的频率）。它们使用 Winstone 基准来比较。因此，例如，具有 Pentium75 性能的处理器被标准 PR75。

[0370] 以下是具有时钟速度的 PR 表格：

[0371]

处理器	以 MHz 计的内部/外部时钟速度
NexGen Nx586-PR75	70 / 35
NexGen Nx586-PR80	75 / 37,5
NexGen Nx586-PW0	84 / 42
NexGen Nx586-PR100	93 / 46,5
NexGea Nx586-PRl IO	102 / 51
NexGen Nx5 86-PR 120	111 / 55,5
AMD Am5x86-PR75	133 / 33
AMD K5-PR75	75 / 50
AMD K5-PR90	90 / 60
AMD KS-PRl 00	100 / 66
AMD K5-PR120	90 / 60
AMD KS-PR133	100 / 66
AMD KS-PRl66	116,7 / 66
AMD K5-PR200	133 / 66
Cyrix 5x86-PR75	100 / 33
Cyrix 5x85-PR90	120 / 40
Cyrix 6x86-PR90	80 / 40
Cyrix 6x86-PR120	100 / 50
Cyrix 4x86-PR133	110 / 55
Cyrix 6x86-PRI 50	120 / 60
Cyrix 4x86-PR166	133 / 66
Cyrix 4x86-PR200	150 / 75
Cyrix 6x 86MX-PR133	100 /50, 110 / 55
Cyrix 6x86MX-PR150	120 /60, 125 / 50
Cyrix 6x86MX-PRl66	133 /66, 137,5 / 55, 150 / 50
Cyrix 6x86MX-PR200	150 / 75, 165 / 55, 166 / 66
Cyrix 6xX6MX-PR233	166 / 83, 187,5 / 75, 200 / 66
Cyrix 6xX6MX-PW66	207,5 / 83, 225 / 75, 233 / 66
Cyrix M-II: PR300	207,5 / 83, 225 / 75, 233 / 66
Cyrix M-Il PR333	250 / 83
Cyrix M-11 PR366	250 / 100
Cyrix M-H PR400	285 / 95
Cyrix M-I1 PR433	300 / 100
Rise mP6-PRl66	1 66 / 83
Rise mP6-PR233	190 / 95
Rise mP6-PI266	200 / 100
Rise mP6-PR333	237,5 / 95
Rise mP6-PR366	250 / 100
DT WinChip2A-PR200	200 / 66
DT WinChip2A-PR233	233 / 66
IDT WinChip2A-PR300	250 / 100
IDT WinChip3-PW33	200 / 66

[0372] 特征

[0373] 下面列出了具有 CPUID 指令的处理器特征。存在用户的一些感兴趣的特征：

[0374] 处理器包含浮点单元

[0375] 这个项目表示直接在芯片上存在浮点单元 (FDU),所有的现代 CPU(从 486DX 开始)将包括所述浮点单元。所述 FPU 用于实数计算。

[0376] 时间标记计数器 TSC 提供了在 PC 上的最精确的定时方法;其允许精确地测量处理器频率。

[0377] 多处理器支持(芯片包含 APIC)。这表示存在 APIC,其允许对称多处理。如果这样项目被删去,则 APIC 或者被禁止或者不被支持。

[0378] 处理器序号表示序号被使能。这个有争议的特征可以被禁止,(因此这个项目被删去)可以从 Intel 获得用于这个目的的软件。

[0379] MMX 技术表示处理器指令集扩展。57 个新的 MMX 指令加速图形和多媒体处理。其随着 Intel 的 Pentium MMX 处理器被引入。当前,MMX 被所有的处理器制造商支持。

[0380] 快速保存和恢复 FP/MMX/SSE 表示这个处理器能够迅速地在 FPU、MMX 和 SSE 模式之间转换。

[0381] Intel 流 SIMD 扩展 (SSE) 表示存在第二指令集扩展——70 个新的指令,其加速 3D 图形、声音和因特网的处理。从 Intel 的 Pentium III 处理器向上支持。

[0382] 接着的几个特征仅仅被与 Intel 竞争的处理器支持:

[0383] 部分 SSE 支持表示 Athlon(和更新的)处理器的指令集扩展。其支持 SSE-MMX 和 SSE-MEM 指令。

[0384] Cyrix 扩展 MMX 表示用于 6x86MX2 M-I1 和更新的处理器的指令集扩展。这些处理器支持一些新的 MMX 指令。

[0385] AMD 3Dnow ! 表示对于从用于 3D 图形加速的 AMD(其首先随着 KS-2 处理器被引入)起的 23 个指令的支持。这个图形指令集也被 IDTWinChipclq 支持。AMD 扩展 3Dnow ! AMD Athlon(和更新的)处理器具有附加的 3D 指令。

[0386] 存储器

[0387] MOV 测试是两个存储器基准的第一个,其测量存储器和高速缓冲存储器的传送速度。通过将同一数据块传送两次来测量这些存储器速度。在第一次传送期间,数据块被安装到高速缓冲存储器中;第二次,时间被从所述高速缓冲存储器传送。所述快尺寸从 2kB 向 2MB 重复地增加。传送速度在特定的块尺寸之上相当大地降低,用于表示高速缓冲存储器已经达到了全部容量。可以以这种方式来检测高速缓冲存储器大小。可以在这个测试中使用一对 MOV 指令一最常用的指令之一。但是,使用一个 MOV 指令的传送慢于经由 MOVSD 指令的传送,其用于我的第二存储器测试。

[0388] 在此是用于这个传送的一对示例源代码:

[0389] @rcpeat :mov eax,[esi]

[0390] mov[edij,eax

[0391] add esi,4

[0392] add edi,4

[0393] dec ecx

[0394] jnz@repeat

[0395] EST 包含源地址,ED1 保存目标地址,ECX 包含重复次数。为了传送 4K,需要 1024

次重复，因为一次传送 32 比特（4 字节）。指令 MOVEAX、[ESI] 从在存储器中的源地址 [ESI] 向在处理器中的 EAX 寄存器中读取数据。第二指令 MV[EDI]、EAX 从 EAX 向在 [EDI] 中的存储器中的目标地址写回数据。接着的两个指令 ADD ESI，4 和 ADD EDX，4 将源和目标递增的指针递增指向我们将传送的下 4 个字节。接着的指令 DEC ECX 将 ECX 寄存器递减 1，以便所述循环将仅仅被重复 1023 次。快速指令 JNZ@WPEAT 强制重复这个循环，直到 ECX 到达 0。

[0396] 高速缓冲存储器是快速和小的。其保存可以在高速缓冲存储器中迅速访问的频繁使用的数据，高速缓冲存储器在 386 母板上被第一次使用。从 486 处理器开始，使用两个高速缓冲存储器。存在：第一级高速缓冲存储器 (L1)，其在芯片上；第二级高速缓冲存储器 (L2)，其通常在母板上。这个第二级高速缓冲存储器更大，但是比另一个更慢。在 Pentium 类处理器中，第一级高速缓冲存储器被划分为代码和数据高速缓冲存储器。

[0397] 一些在管芯上的高速缓冲存储器大小：

[0398]

处理器	L1 高速缓冲存储器	L2 管芯上的高速缓冲存储器
Intel i486SX/DXDX2	8 kB	
Intel i4 86DX4	16 kB	256 kb to 1 MB
Intel Pentium	16 kB(8 kB+8 kB)	512 kB (Xeon to 2 MB)
Intel Pentium MMX	32 kB(16 kB+ 16 kB)	
Intel Pentium Pro	32 kB(16 kB+ 16 kB)	128 kB
Intel Pentium II/III	32 kB(16 kB+ 16 kB)	256 kB
Intel Celeron	32 kB(16 kB+ 16 kB))	
Intel Celeron A	32 kB(16 kB+ 16 kB)	256 kB
Intel Pentium III E	32 kB(16 kB+ 16 kB)	512 kB
AMD Am486DX/DX2/DX4	8 kB	
AMD Am5x86	16 kB	
AMD K5	24 kB (16 kB + 8 kB)	
AMD K6/K6-2	64 kB (32 kB + 32 kB)	
AMD K6-III	64 kB (32 kB + 32 kB)	
AMD Athlon	128 kB (64 kB + 64 kB)	
Cyrix Cx486SLC/DLC	1 kB	
Cyrix Cx486S	2 kB	
Cyrix Cx486DX/DX2/DX4	8 kB	
Cyrix 5x86/6xS6	16 kB	
Cyrix 6x86MX/M-II	64 kB	
IDT WinChip/WinChip2	64 kB (32 kB + 32 kB)	
IDT WinChip3	128 kB (64 kB + 64 kB)	
Rise mP6	16 kB (8 kB + 8 kB)	
NexGen Nx586	32 kB (1 6kB + 16 kB)	
NexGen Nx686	48 kB (8 kB + 8 kB)	
UMC 486	8 kB	
IBM 486SLC	16 kB	

[0399] 存储器 2

[0400] MOVSD 测试与第一存储器基准类似地工作。其也分别测量存储器传送速度、高速缓冲存储器传送速度，但是使用 MOVSD 指令。这个指令比一对 MOV 指令更快，因为调制解调器处理器将使用突发周期预先获取读取和将数据组合写入突发周期中。传送数据块的方法是类似的：ESI 包含源地址，ED1 保存目标地址，ECX 计数重复次数。然后执行 REPMOVSD 指令。REP 前缀表示将重复地执行下面的指令。在 ECX 寄存器中确定重复次数，ECX 寄存器的值在

每个迭代被减少，直到所述值是 0。然后 REP MOVSD 的执行结束。MOVSD 指令将数据从源地址 [ESI] 向目标地址 [EDI] 一对，并且提高两个指针 (ESI 和 EDI) 以指向下一个位置。

[0401] 计算

[0402] 下面列出 5 个数学基准：

[0403] 第一基准使用整数来计算大阶乘积，因此这个基准仅仅使用处理器（不使用 FPU)。阶乘积 10001 是从 1 到 10001 的所有数字的乘积：

[0404] 10001 ！ ＝ 1*2*3*...9998*9999*10000*100001

[0405] 这个阶乘积结果被存储在存储器的 14812(超过 14 k3) 字节中 -118496 比特数量！结果将仍然适配进在大多数处理器中的管芯上的 L1 高速缓冲存储器中。其将不反映主存储器性能。

[0406] 第二基准计算前 30000 个素数。这个基准仅仅再次使用整数，因此它仅仅测试处理器，并且使用大约 120Id3 存储器，其仅仅被访问一次。不需要高速缓存。

[0407] 存在多个智能算法来确定素数，我们可以使用下面的算法：

[0408] 如果数量 n 不可被大于 1 的数量和小于 n 的数量整除，则数量 n 是素数。但是其将足以被数量（或者因子）hm2 到数量 a 的平方根整除。在 2 之外的所有的偶数不能是素数，因此按照定义，它们可以被数量 2 整除。

[0409] 第三基准使用拉普拉斯变换来计算 9x9 矩阵的行列式。这个基准与实数的（正则）矩阵一起工作，因此它将使用处理器和 FPU。拉普拉斯变换基于将原始矩阵分解为更小的行列式，它们然后被分解等，直到获得单个数量。在 TestCPU 中，这是通过递归的过程调用进行的。在此是作为在数学项上这个基准的示例的分解 3x3 矩阵。

[0410] 检测用户的调制解调器速度

[0411] 不幸的是，没有简单的方式来仅仅调用一个函数，并且发现用户的因特网连接的精确的速度。这样做的唯一的现实方式是从因特网下载大文件，然后监控所述下载的进程。通过根据下载的大小测量下载文件所需要的时间，你可以计算用户的连接速度的估计值（这恰好是大多数浏览器下载功能所做的事情）。更重要的是，这种计算不仅仅是理论上的连接速度（即 56Kbps 或者 1.5Mbps)，它是在用户的计算机和你的因特网存在环境之间的真实世界测试。

[0412] 但是，如果大多数用户必须坐等不必要的下载，则他们将被非常烦扰，正是如此，你知道它们的连接速度是怎样的。因此，围绕其的方式是将这个监控查看并入安装器电影中，所述安装器电影预先安装要提供到用户的鉴权界面的实际下载。以这种方式，我们可以获得不烦扰用户的用户连接速度的感觉。

[0413] 当你点击每个按钮时，你将看到被预先安装到你的高速缓冲存储器中的文件的进程。当其预先安装时，其也：计算你在你个人的机器上正在获得的适当下载速度。现在，让我们对于这个下载查看在 Flash 中的采样代码。

[0414]
```
on mouseUp me
```

[0415]
```
preloadFile(" http://www.bharosa.com/test/larg.png" )
```

[0416]
```
end
```

[0417] 这个代码调用 preloadFile 处理器，并且将其传送到精确的 URL 以下载。现在，你需要在你的电影脚本之一中建立 preloadFile 处理器。其代码看起来如下：

```
[0418]      global gNetD,gStartTime
[0419]      on prelaodFile whichFile
[0420]      gNetID = preloadNetThing(whichFile)
[0421]      sStartTime = 0
[0422]      timeout(" checkDownload" ).new(100,#checkDownload)
[0423]     end
```

[0424] 这个 preloadFile 处理器使用两个全局变量 :gNetID 和 gStartTime。第一全局的 gNetID 跟踪当前正在预先安装哪个网络操作。第二全局的 gStartTime 跟踪开始下载的时间。这个处理器通过向 gNetID 分配网络操作 preloadNetThing 的值而开始。接着,其通过将 gStartTime 设置为 0 来将其初始化。最后,它建立超时对象,其将在每 100 毫秒或者大致每秒 10 次调用处理器 checkDownload。网络查看器将每秒 10 次地执行 checkDownloadhandler。这个处理器看起来如下 :

```
[0425]  on checkDownload
[0426]   tempStatus = getSmamStatus(gNetID)
[0427]   case tempStatus.state of
[0428]   " Complete" :
[0429]   timeout(" checkDownload' ).forget 0
[0430]   " Started" , " InProgress" :
[0431]   if gStartTime = 0 then
[0432]     gStartTime = the ticks
[0433]    end if
[0434]    end case
[0435]    sendAllSprites(#updateDownloadInfo,tempStatus.bytesSoFar.
[0436]   tempStatus.bytesTotal,
[0437]     gStartTime)
[0438]  end
```

[0439] 这个处理器通过获取我们较早调用的预先安装操作的 streamStatus 而开始。在网络查看器中的 getstreamStatus 功能返回在 Checker 中的属性,其看起来如下 :

[0440] 在这个列表中存在 5 种不同的属性。#url 属性告诉我们正在下载的精确的 URL,#状态属性告诉我们下载正在发生什么。状态值有 5 个不同的可能 :“Connecting(连接)”、“Started(开始)”、“InProgress(在进展中)”、“Complete(完成)”和“Error(错误)”。#bytesTotal 属性告诉我们在下载中的字节的总数。最后,如果存在错误,则其在 #error 属性中被返回。

[0441] 在 checkDownload 处理器中,我们向本地的变量名 tempStatus 分配这个属性列表。接着,我们查看 #state 属性的值,如果所述操作已经完成,则我们忘记所述超时对象,并且全部完成。如果 #state 刚刚开始或者在进行中,则我们查看是否全局变量 gStartTicks 仍然被设置为 0。如果是,则我将其值重新设置为 ticks,其是与一秒的 1/60 为单位的当前时间相关联的系统属性。最后,我们使用 sendAllSprites 命令来调用在进行中的不同子图形的每个中的 updateDownloadInfo 处理器。

[0442] 在进程条和包含当前时间的文本字段上有不同的动作，这些动作使用别发送到其的信息来更新它们自己的内容。但是，最重要的事情是你使用这个信息来计算平均现代速度。那个代码看起来如下：

[0443] on updateDownloadInfo me,bytesSoFar,bytesTotal,startTicks

[0444] if startTicks<>0and bytesTotal<>0 then

[0445] tempTime = (the ticks-startTicks)/60.0

[0446] if tempTime<>0then

[0447] modemRate = ((bytesSoFar*8.0)1 1000.0)/tempTime

[0448] sprite(mc.spriteNum).member.text = string(modemRate)&&" Kbps"

[0449] end if

[0450] end if

[0451] end

[0452] 这个处理器通过保证 startTicks 和 bytesTotal 不等于 0 而开始，这有效地保证所述下载已经实际上开始。接着，它从 startTicks 减去当前的 ticks，并且将数量除以 60 以给出自从下载开始起已经过去的精确的秒数。如果 tempTime 不等于 0，则这个处理器通过下述方式来计算 modemRate：通过获取迄今的字节，将其乘以 8，然后将其除以 1000。其然后将那个数量除以自从下载开始已经过去的总的秒数，则你获得实际的下载速度。最后，获取这个数量，并且将其显示在屏幕的文本成员中。

[0453] 因此用于调制解调器速度的这个公式如下。被发送到处理器的数量是已经下载的字节的总数。但是，传统的调制解调器速度以比特表示，而不是以字节表示，因此我们需要将字节的数量乘以 8 以获得比特的数量。接着，调制解调器速度以千比特为单位，因此为了获得那个数量，我们获取比特总数，并且将它们除以 1000。最后，我们要知道每秒的千比特的数量，因此我们获取千比特的总数，并且将其除以总的秒数，以获得每秒的千比特的数量。

[0454] 因此，当进行下载并且我们准备好接着移动到实际鉴权界面（鉴权器）电影时，我们使得文本字段准备好，其包含用户的因特网连接速度的相当精确的说明。

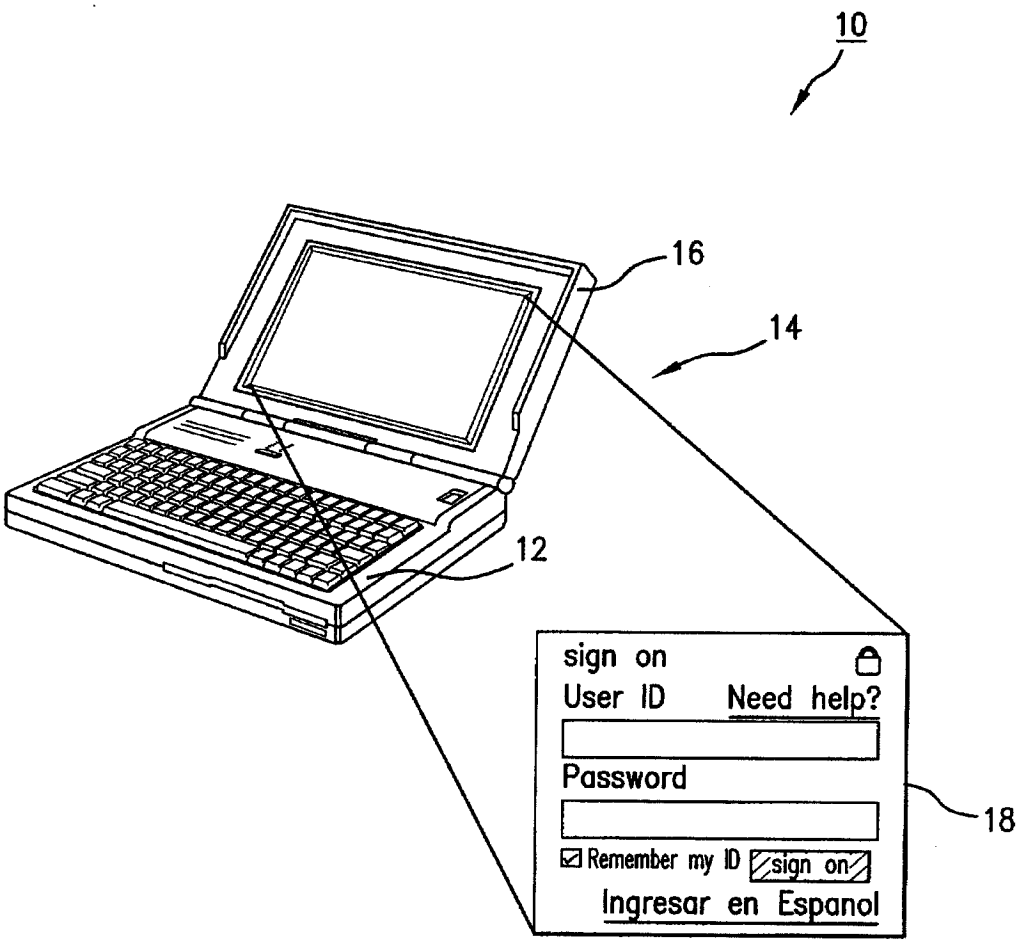

10
16
14
12
sign on
User ID
Need help?
Password
18
Remember my ID
sign on
Ingresar en Espanol

图 1

现有技术

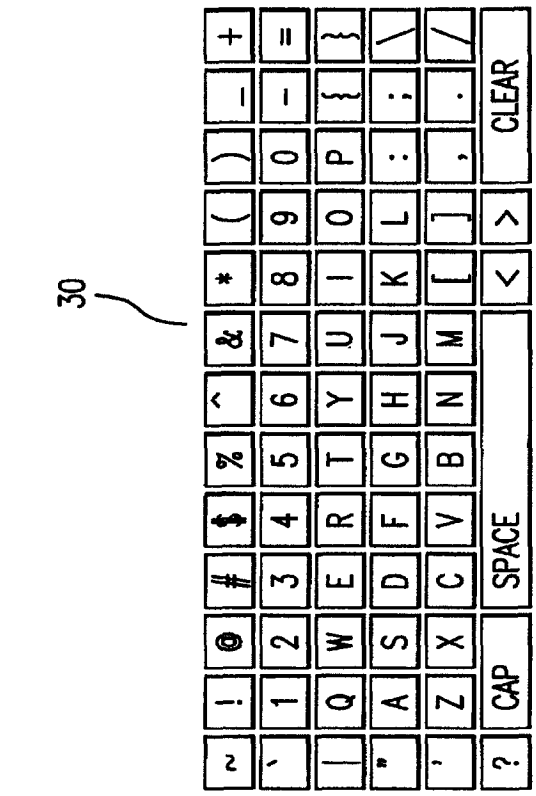


图3

现有技术

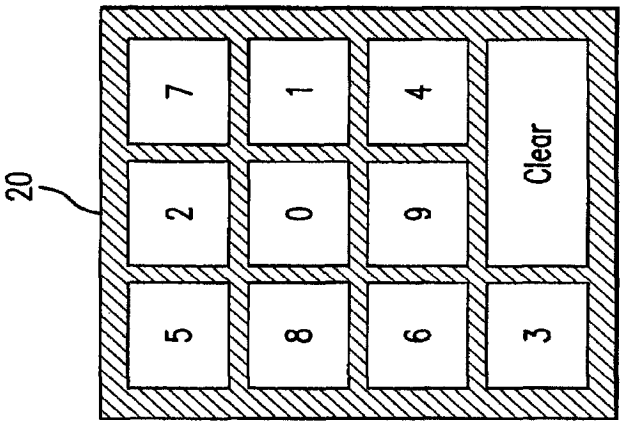


图2

现有技术

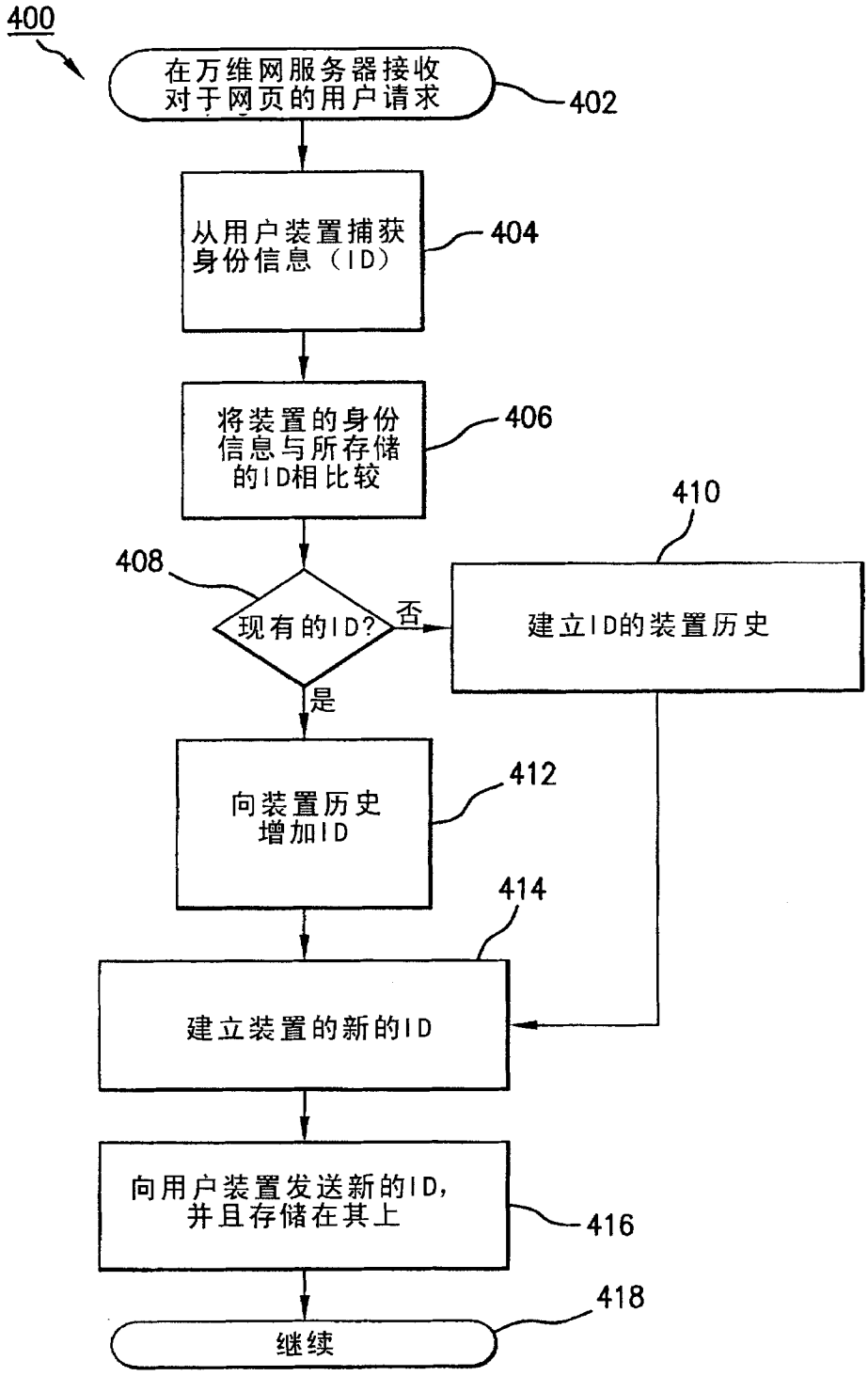

400
在万维网服务器接收对于网页的用户请求
402
从用户装置捕获身份信息（ID）
404
将装置的身份信息与所存储的ID相比较
406
410
408
现有的ID?
否
建立ID的装置历史
是
向装置历史增加ID
412
414
建立装置的新的ID
向用户装置发送新的ID，并且存储在其上
416
418
继续

图 4A

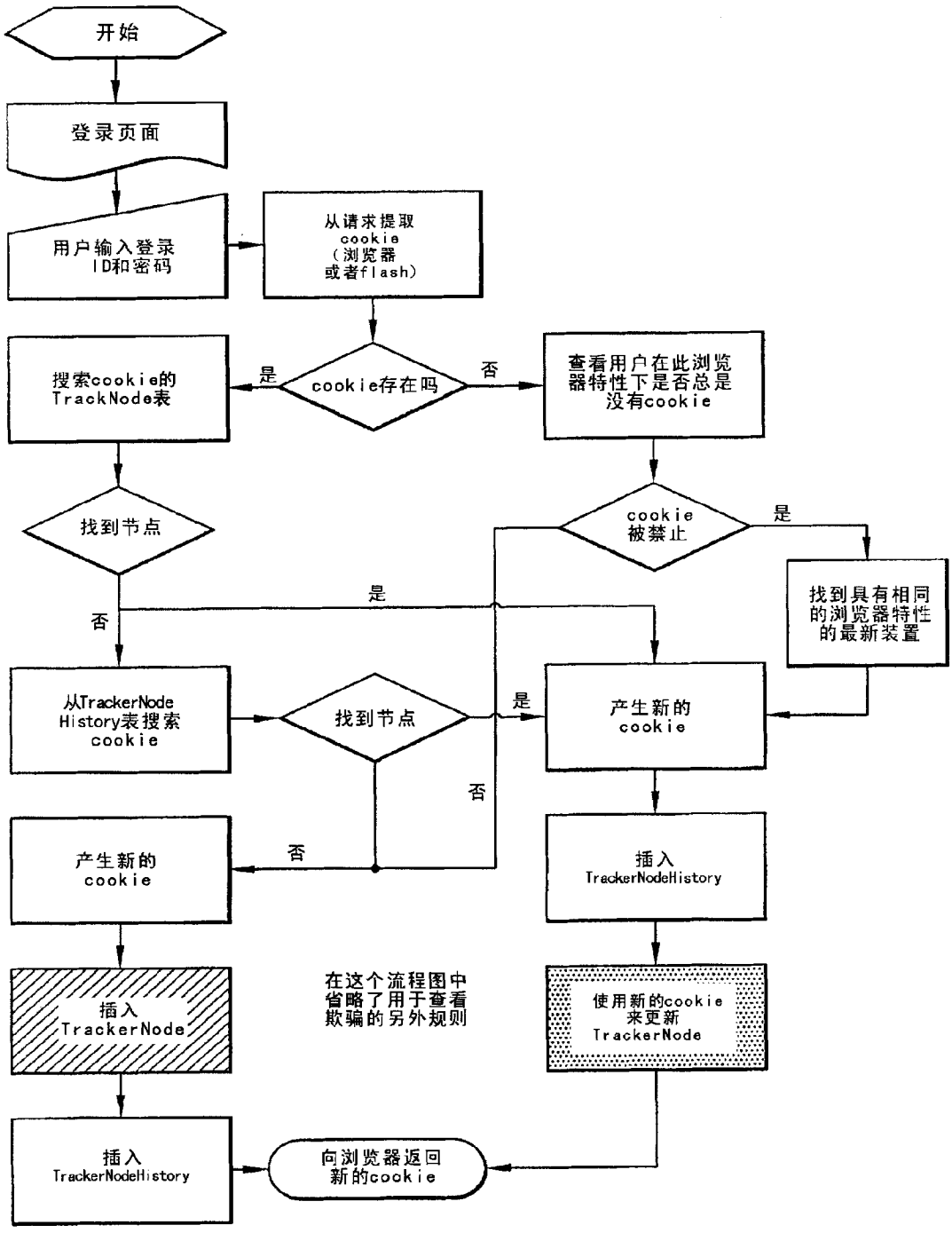

开始
登录页面
用户输入登录ID和密码
从请求提取cookie（浏览器或者flash）
搜索cookie的TrackNode表
是
cookie存在吗
否
查看用户在此浏览器特性下是否总是没有cookie
找到节点
cookie被禁止
是
找到具有相同的浏览器特性的最新装置
否
是
从TrackerNode History表搜索cookie
找到节点
是
产生新的cookie
否
否
产生新的cookie
插入TrackerNodeHistory
插入TrackerNode
在这个流程图中省略了用于查看欺骗的另外规则
使用新的cookie来更新TrackerNode
插入TrackerNodeHistory
向浏览器返回新的cookie

图 4B

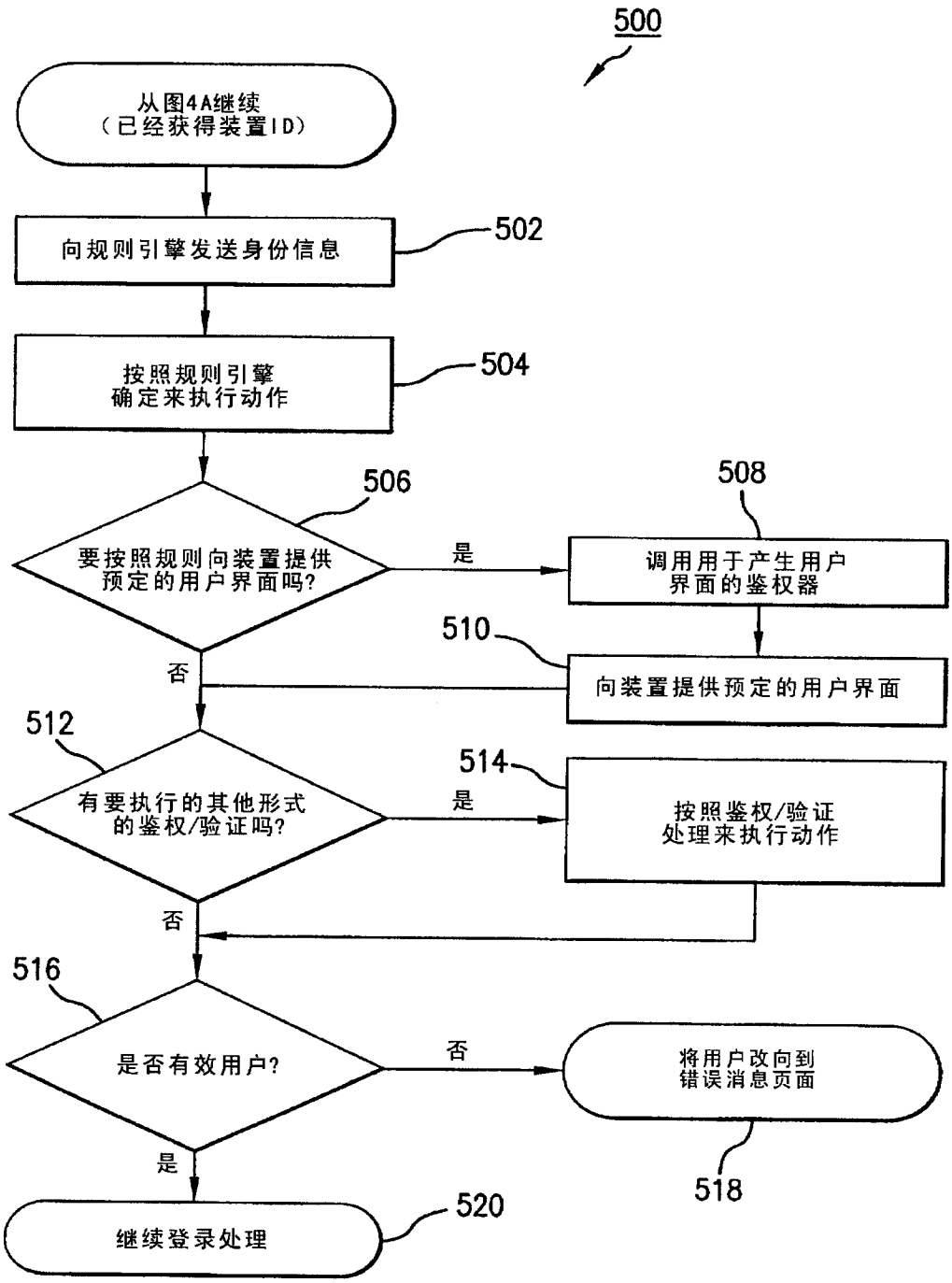

500
从图4A继续
（已经获得装置ID）
向规则引擎发送身份信息
502
按照规则引擎
确定来执行动作
504
506
要按照规则向装置提供
预定的用户界面吗?
是
508
调用用于产生用户
界面的鉴权器
否
510
向装置提供预定的用户界面
512
有要执行的其他形式
的鉴权/验证吗?
是
514
按照鉴权/验证
处理来执行动作
否
516
是否有效用户?
否
将用户改向到
错误消息页面
518
是
继续登录处理
520

图 5

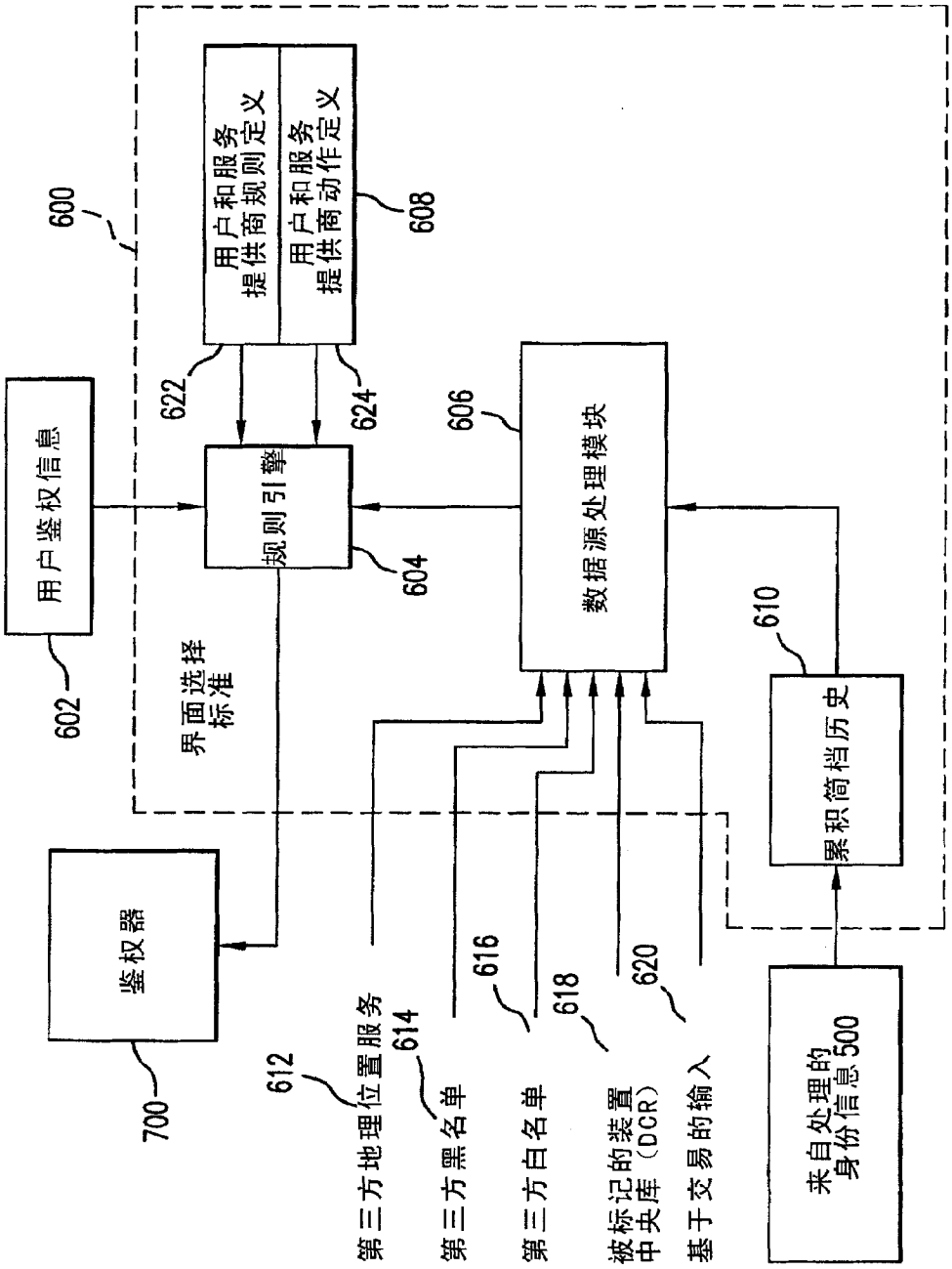

600
用户和服务
提供商规则定义
用户和服务
提供商动作定义
608
622
624
606
用户鉴权信息
规则引擎
604
数据源处理模块
602
界面选择
标准
610
累积简档历史
鉴权器
700
612
第三方地理位置服务
614
第三方黑名单
616
第三方白名单
618
被标记的装置
中央库（DCR）
620
基于交易的输入
来自处理的
身份信息500

图6

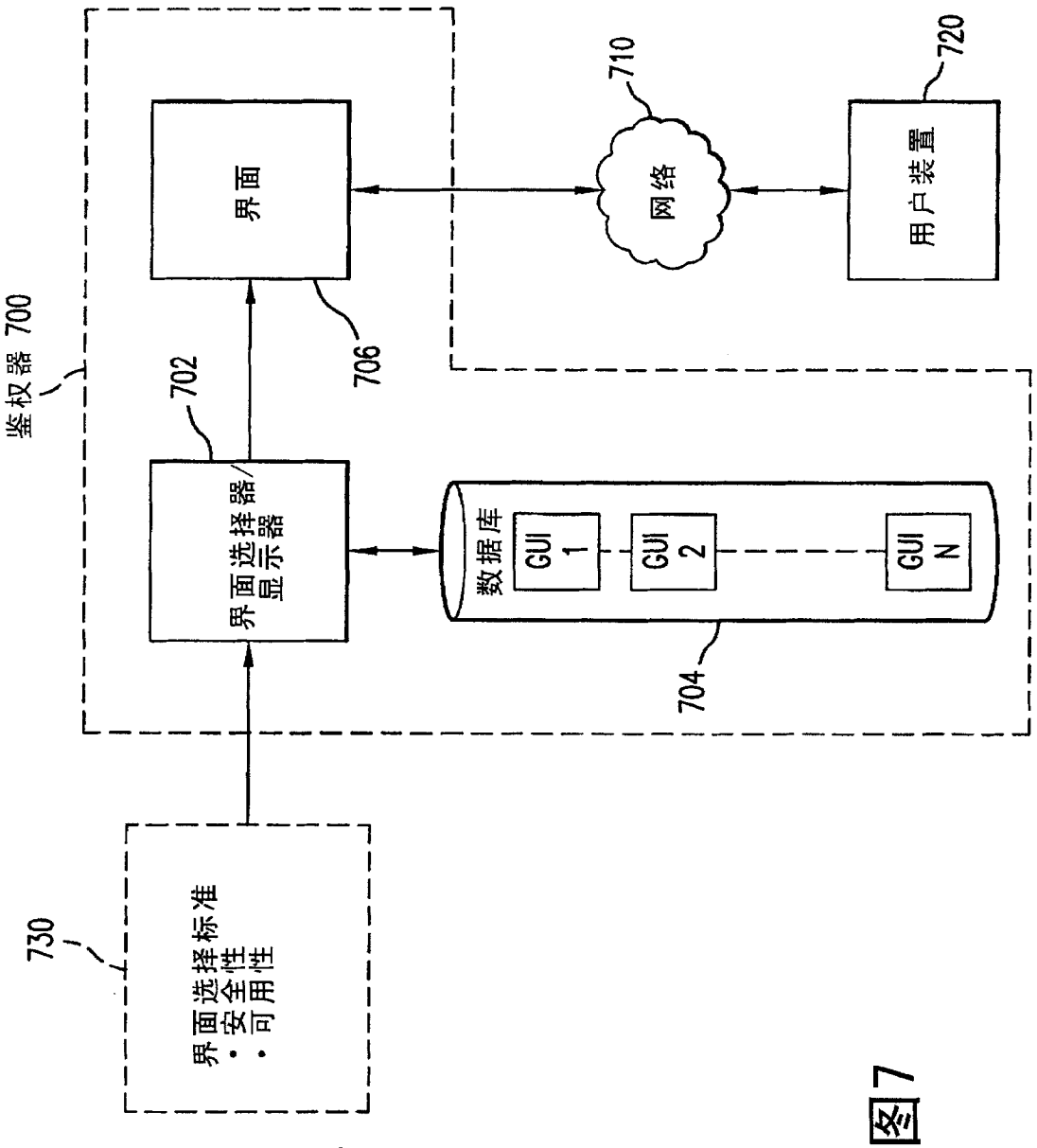

鉴权器 700
界面
网络
用户装置
710
720
706
702
界面选择器/
显示器
数据库
GUI 1
GUI 2
GUI N
704
730
界面选择标准
• 安全性
• 可用性

图 7

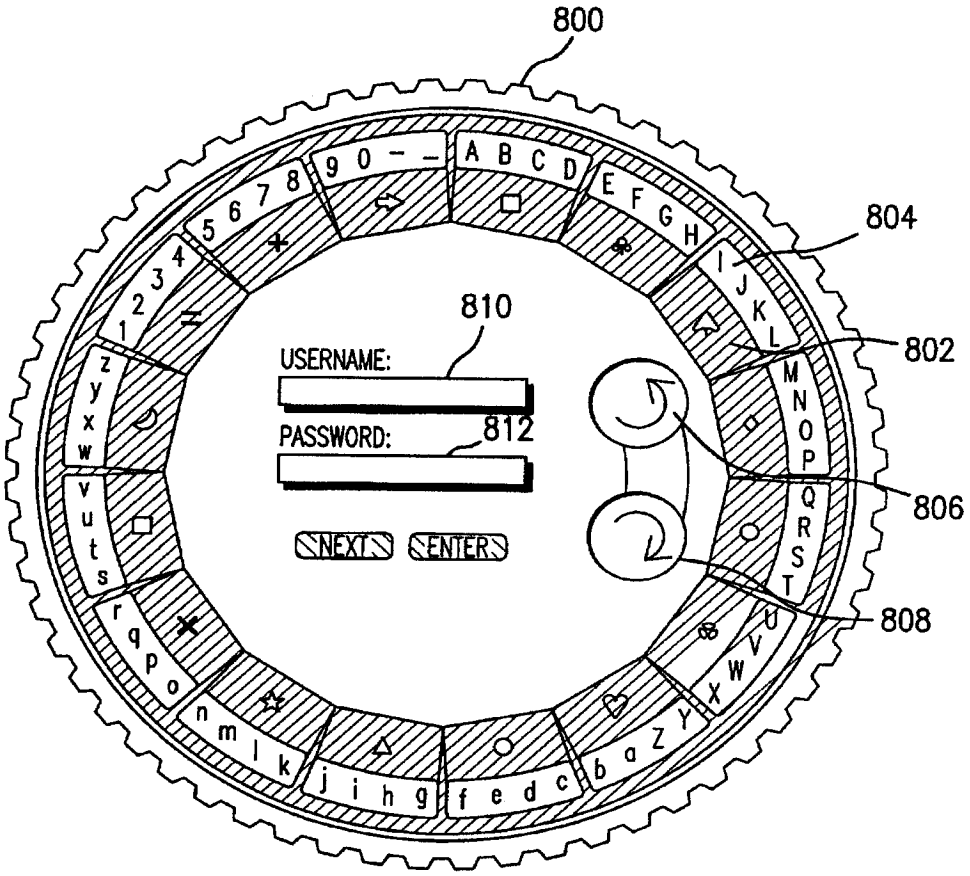


图 8

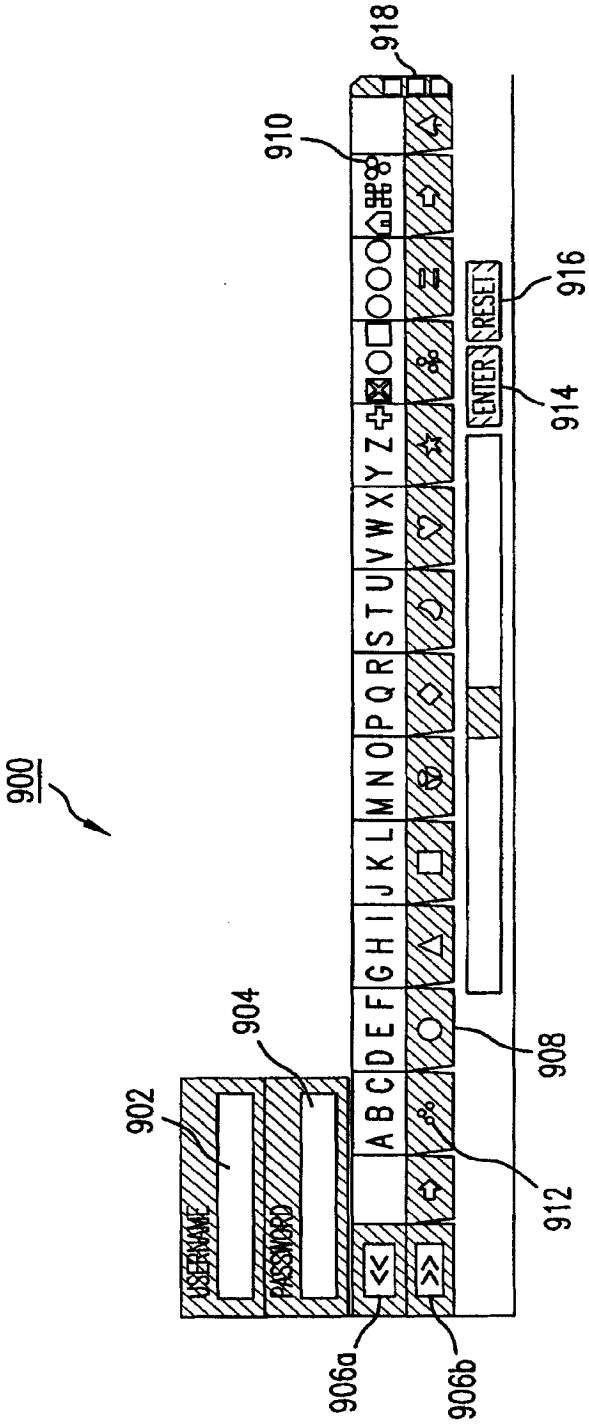

900
902
904
906a
906b
908
910
912
914
916
918
USERNAME
PASSWORD
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
<<
>>
ENTER
RESET

图9

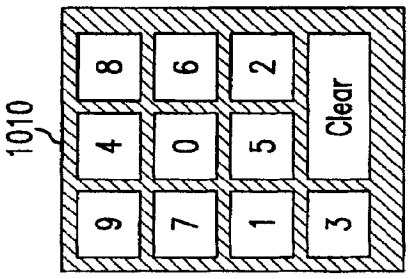


图10A

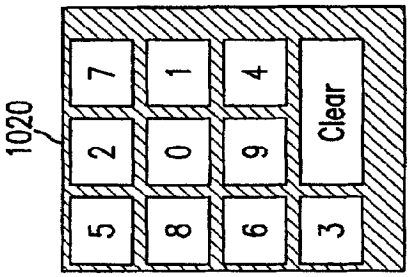


图10B

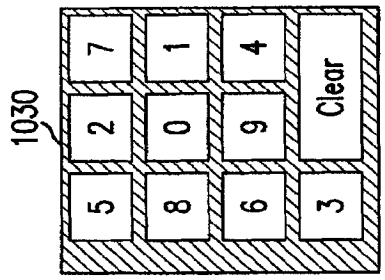


图10C

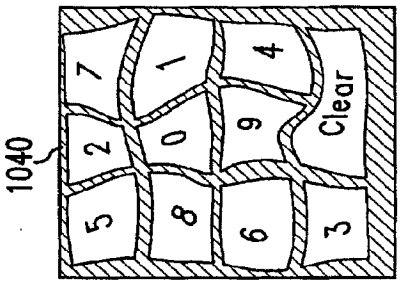


图10D

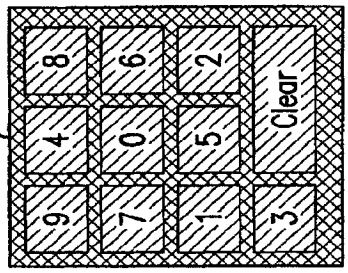


图10E

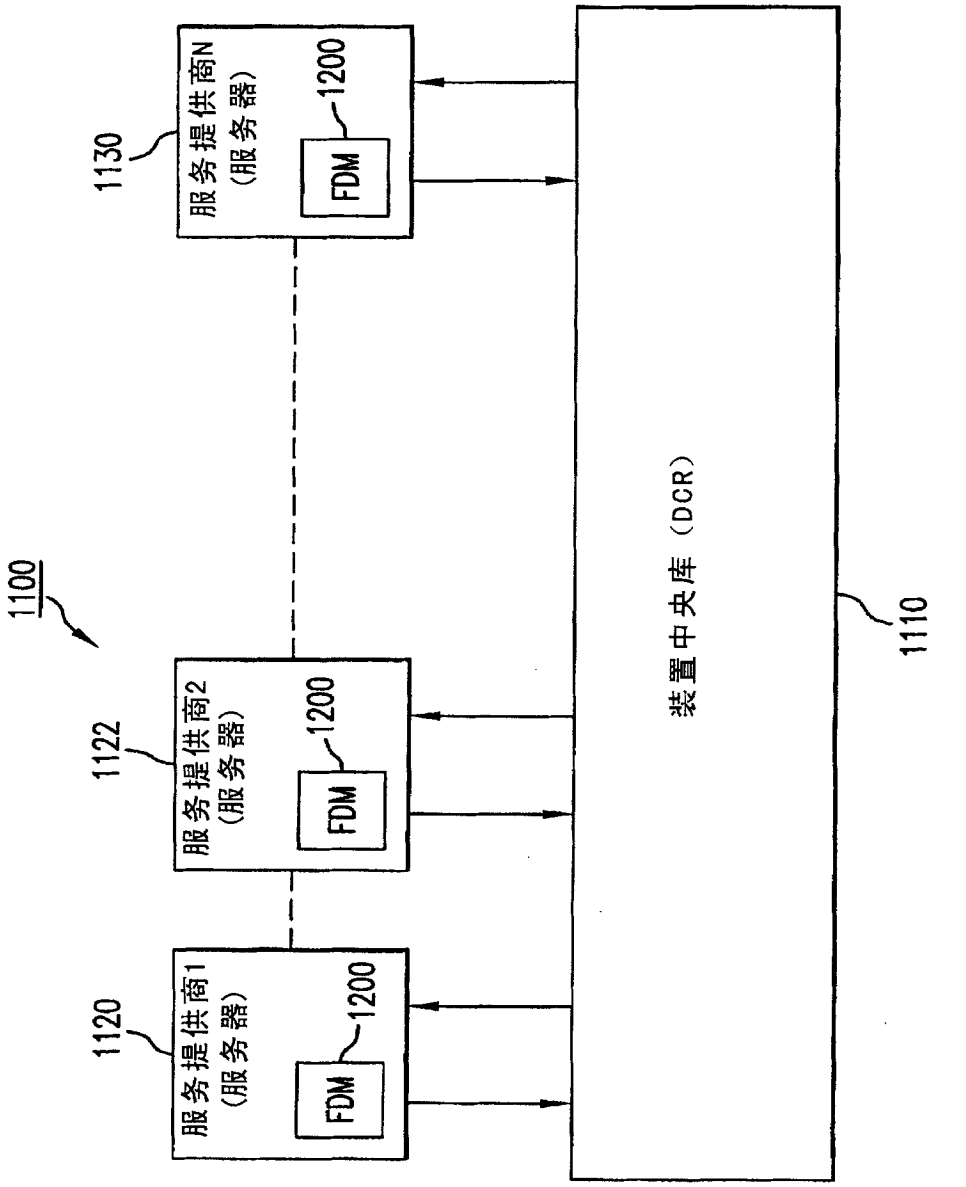

1100
1110
装置中央库（DCR）
1120
服务提供商1（服务器）
1122
服务提供商2（服务器）
1130
服务提供商N（服务器）
FDM
1200

图11

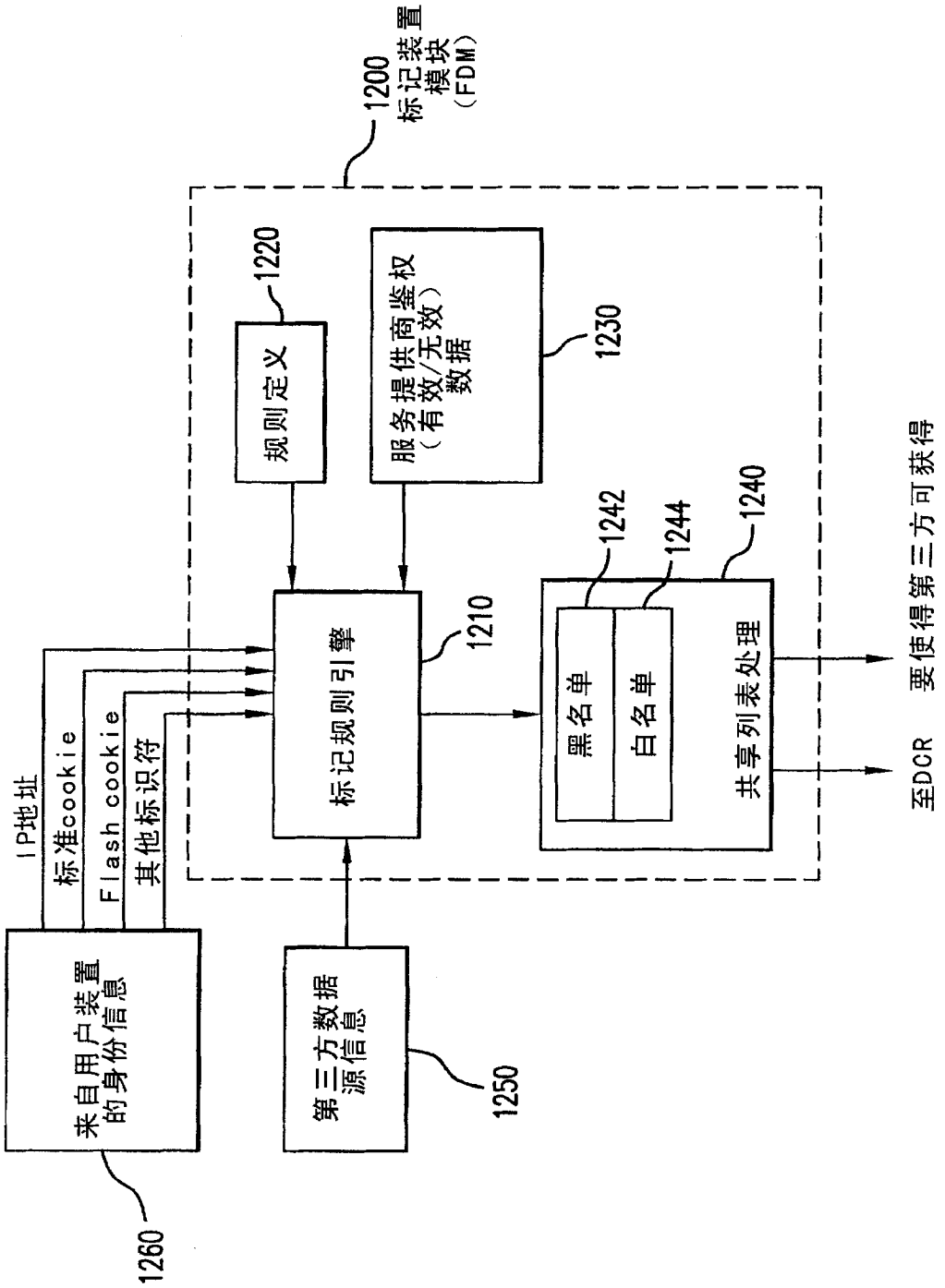

1200
标记装置
模块
(FDM)
1220
规则定义
服务提供商鉴权
(有效/无效)
数据
1230
1210
标记规则引擎
1242
1244
1240
黑名单
白名单
共享列表处理
至DCR 要使得第三方可获得
IP地址
标准cookie
Flash cookie
其他标识符
来自用户装置
的身份信息
1260
第三方数据
源信息
1250

图12

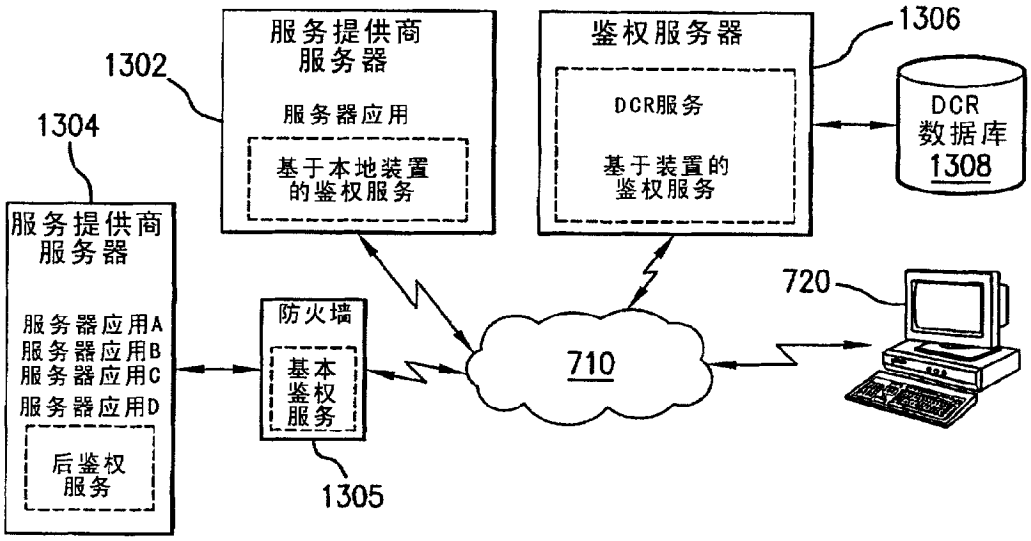

服务提供商
服务器
1302
服务器应用
基于本地装置
的鉴权服务
鉴权服务器
1306
DCR服务
基于装置的
鉴权服务
DCR
数据库
1308
1304
服务提供商
服务器
服务器应用A
服务器应用B
服务器应用C
服务器应用D
后鉴权
服务
防火墙
基本
鉴权
服务
1305
710
720

图 13A

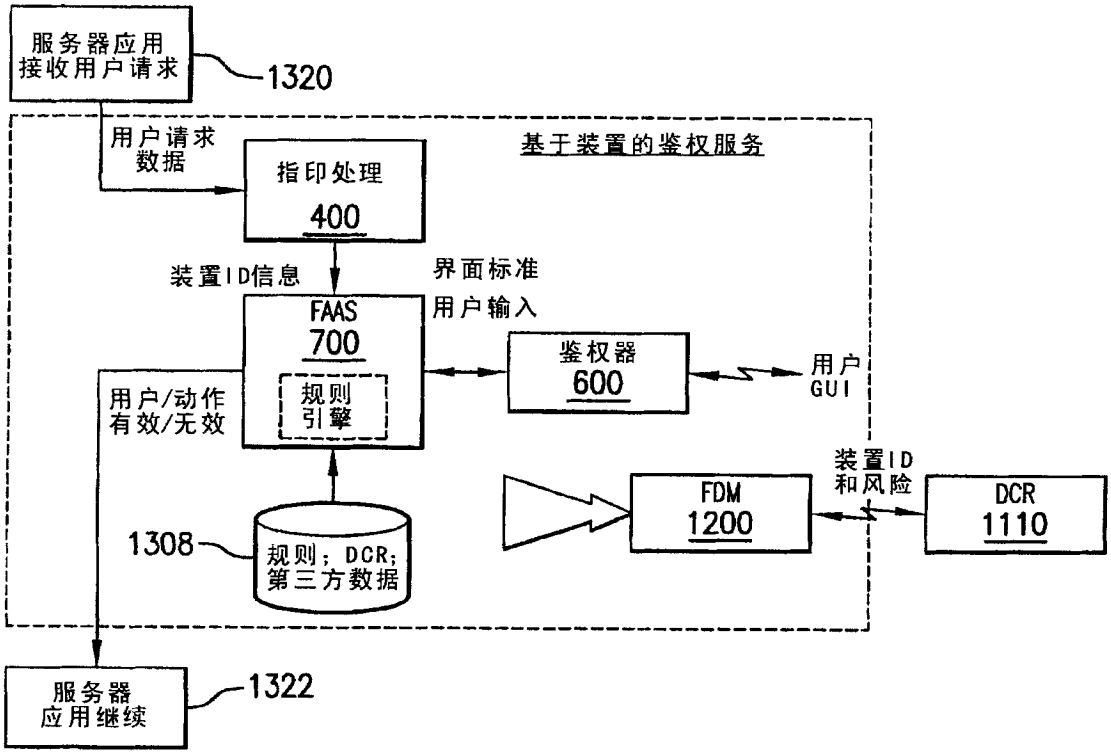

服务器应用
接收用户请求
1320
用户请求
数据
基于装置的鉴权服务
指印处理
400
装置ID信息
界面标准
用户输入
FAAS
700
规则
引擎
鉴权器
600
用户
GUI
用户/动作
有效/无效
装置ID
和风险
FDM
1200
DCR
1110
1308
规则；DCR；
第三方数据
服务器
应用继续
1322

图 13B

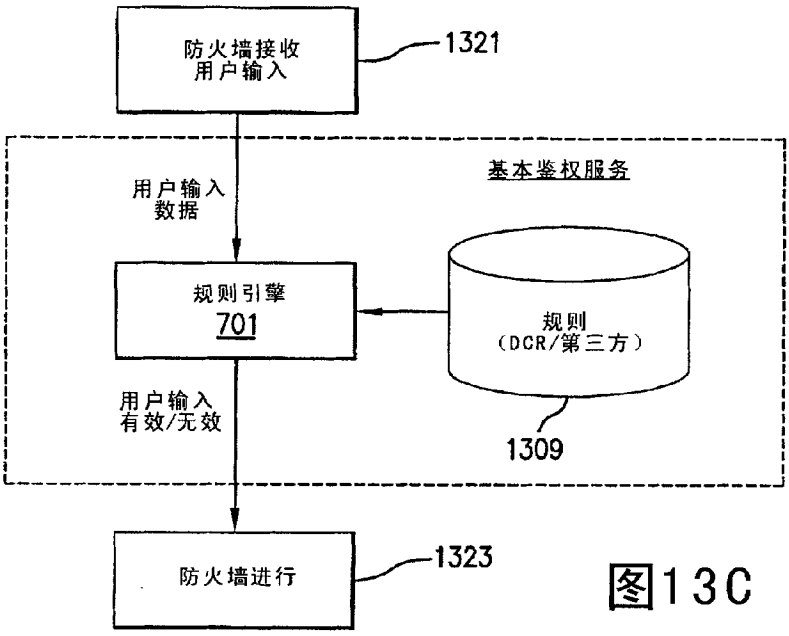

防火墙接收
用户输入
1321
基本鉴权服务
用户输入
数据
规则引擎
701
规则
(DCR/第三方)
用户输入
有效/无效
1309
防火墙进行
1323

图13C

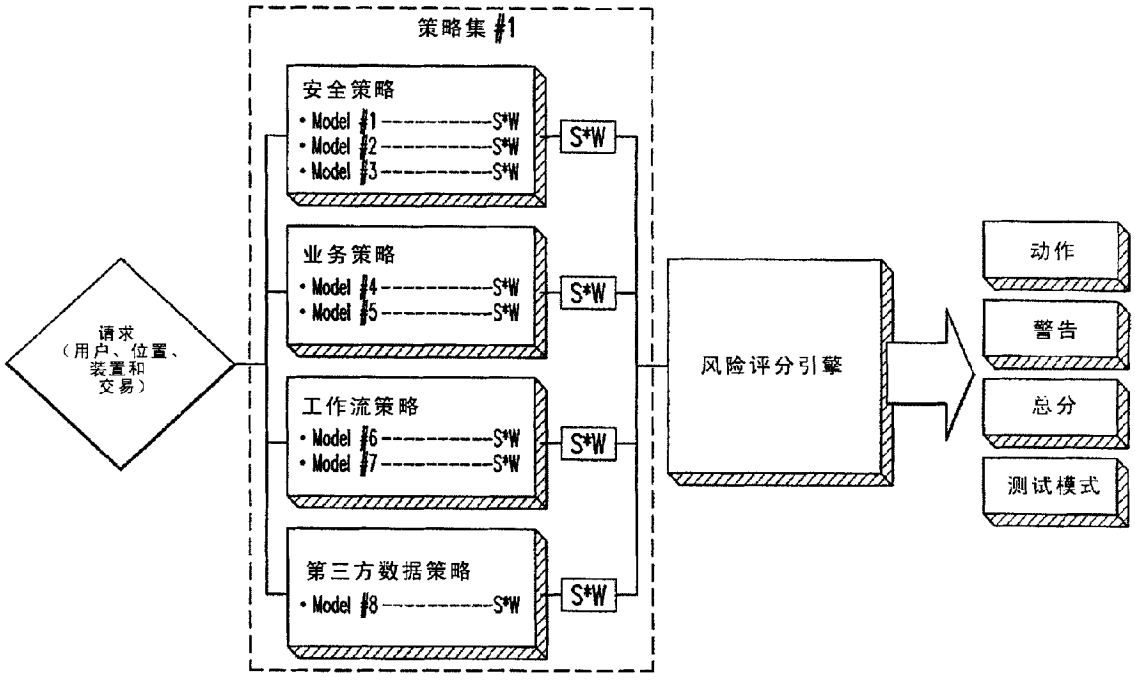

策略集 #1
安全策略
• Model #1 S*W
• Model #2 S*W
• Model #3 S*W
业务策略
• Model #4 S*W
• Model #5 S*W
工作流策略
• Model #6 S*W
• Model #7 S*W
第三方数据策略
• Model #8 S*W
S*W
请求
(用户、位置、
装置和
交易)
风险评分引擎
动作
警告
总分
测试模式

图16C

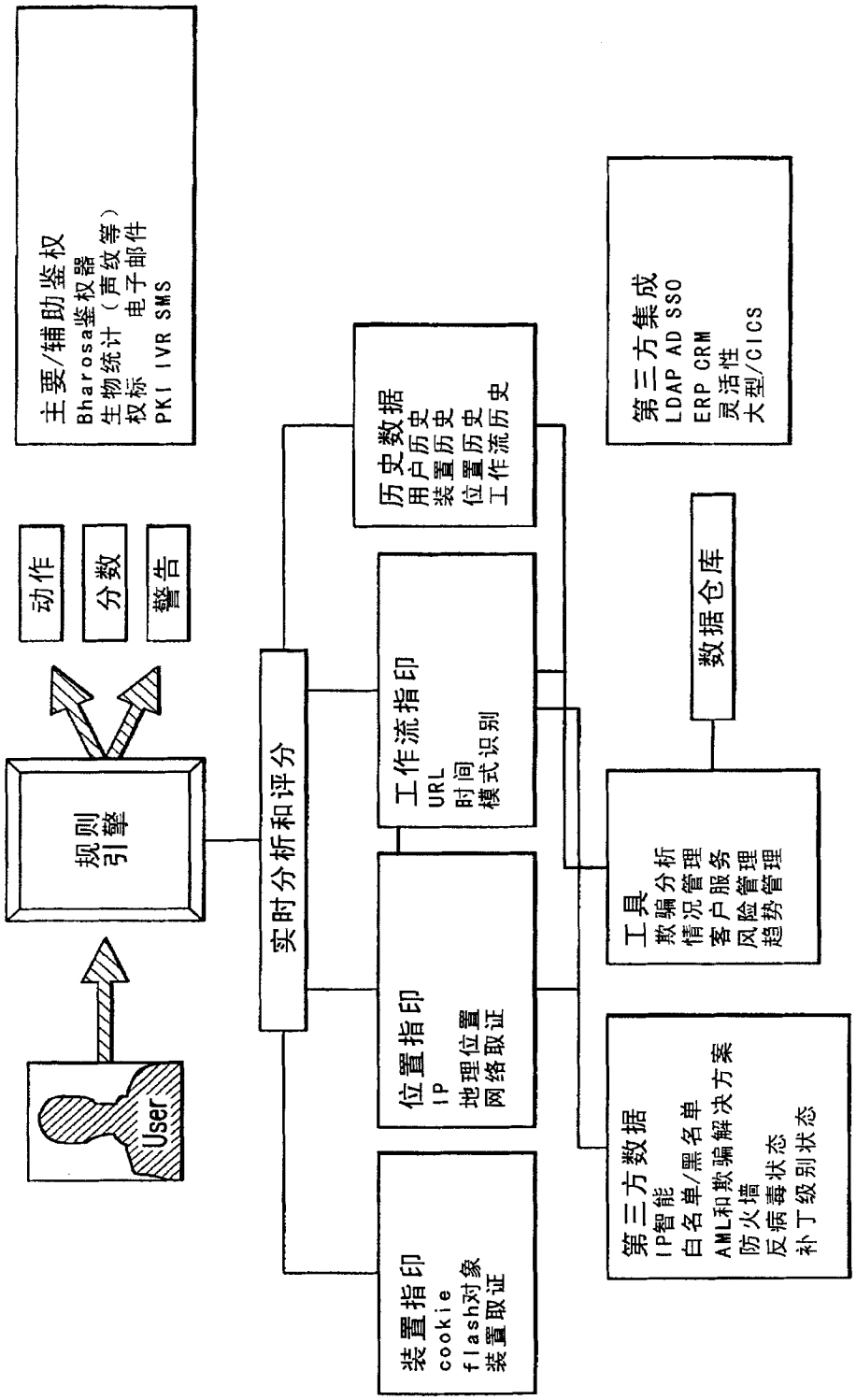

主要/辅助鉴权
Bharosa鉴权器
生物统计（声纹等）
权标 电子邮件
PKI IVR SMS
动作
分数
警告
规则
引擎
User
实时分析和评分
历史数据
用户历史
装置历史
位置历史
工作流历史
工作流指印
URL
时间
模式识别
位置指印
IP
地理位置
网络取证
装置指印
cookie
flash对象
装置取证
第三方集成
LDAP AD SSO
ERP CRM
灵活性
大型/CICS
数据仓库
工具
欺骗分析
情况管理
客户服务
风险管理
趋势管理
第三方数据
IP智能
白名单/黑名单
AML和欺骗解决方案
防火墙
反病毒状态
补丁级别状态

图14

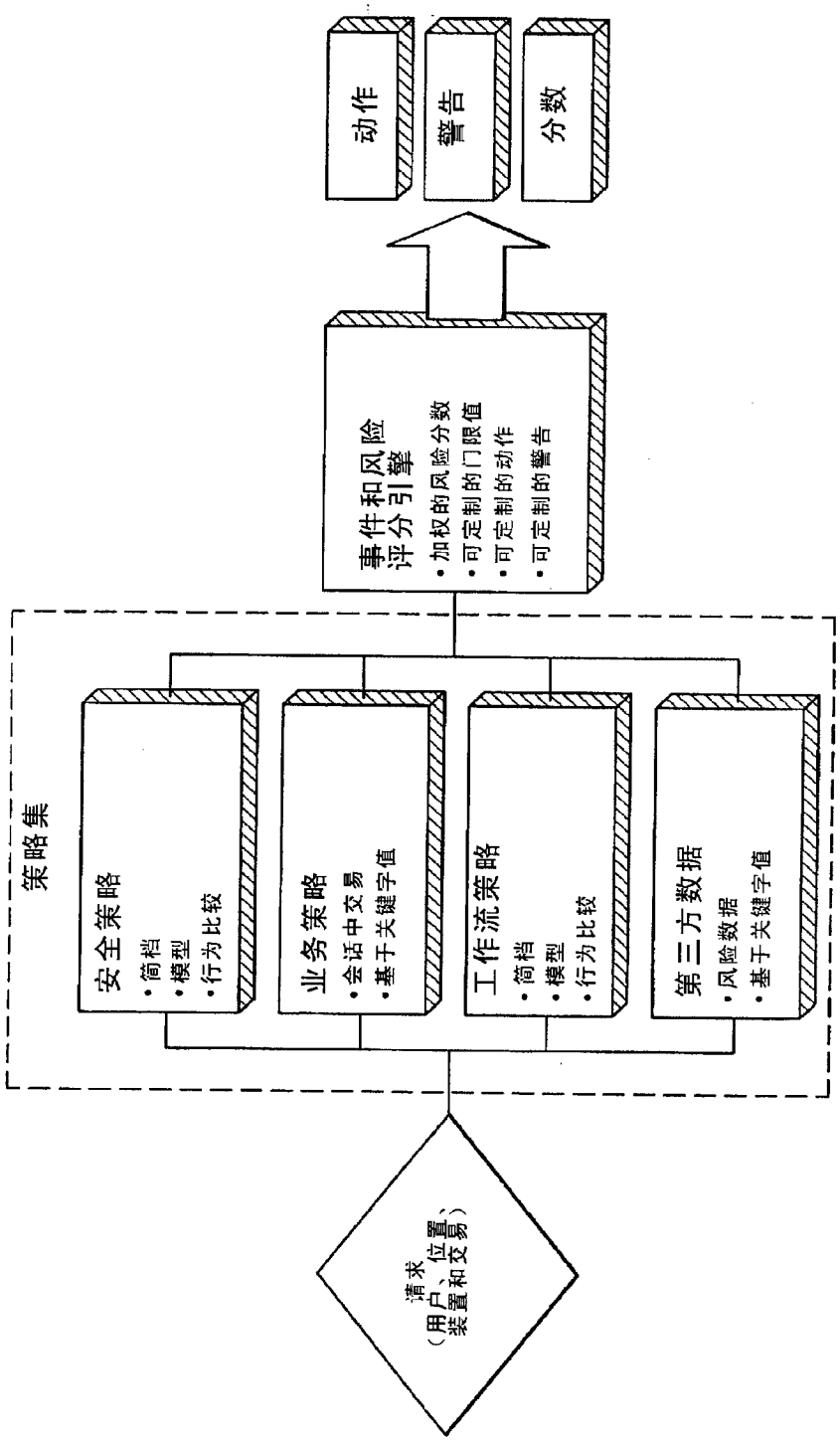

动作
警告
分数
事件和风险评分引擎
• 加权的风险分数
• 可定制的门限值
• 可定制的动作
• 可定制的警告
策略集
安全策略
• 简档
• 模型
• 行为比较
业务策略
• 会话中交易
• 基于关键字值
工作流策略
• 简档
• 模型
• 行为比较
第三方数据
• 风险数据
• 基于关键字值
请求
（用户、位置、
装置和交易）

图15A

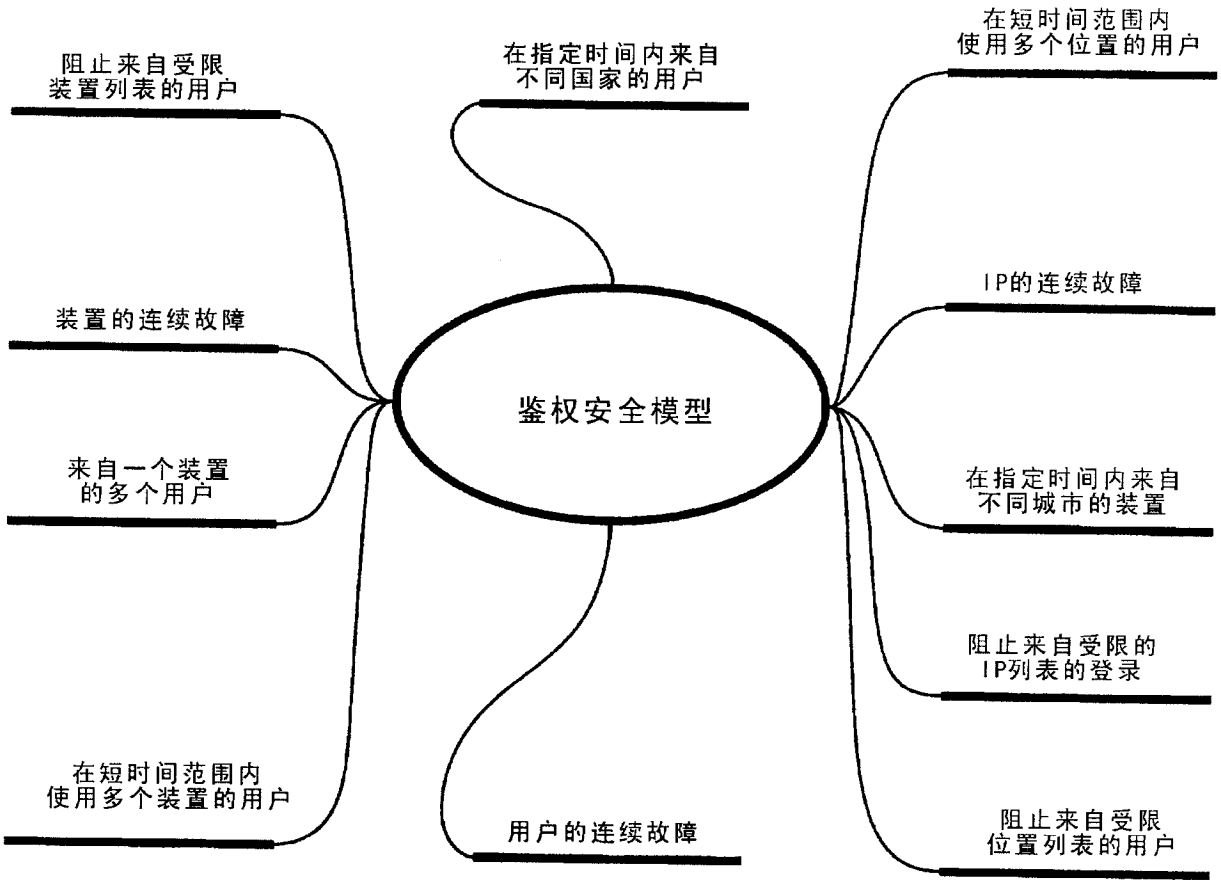

阻止来自受限
装置列表的用户
在指定时间内来自
不同国家的用户
在短时间范围内
使用多个位置的用户
装置的连续故障
IP的连续故障
鉴权安全模型
来自一个装置
的多个用户
在指定时间内来自
不同城市的装置
阻止来自受限的
IP列表的登录
在短时间范围内
使用多个装置的用户
用户的连续故障
阻止来自受限
位置列表的用户

图 15B

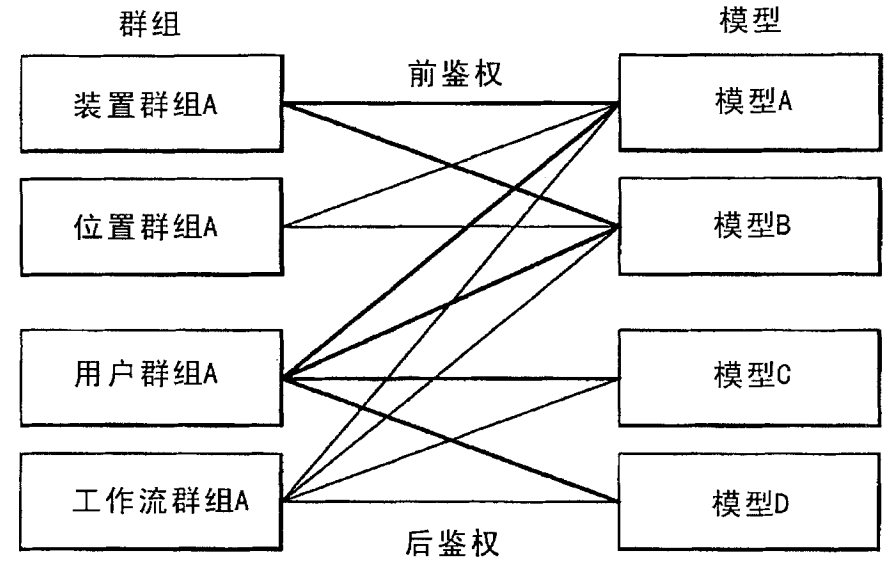

群组
模型
前鉴权
装置群组A
模型A
位置群组A
模型B
用户群组A
模型C
工作流群组A
模型D
后鉴权

图 16A

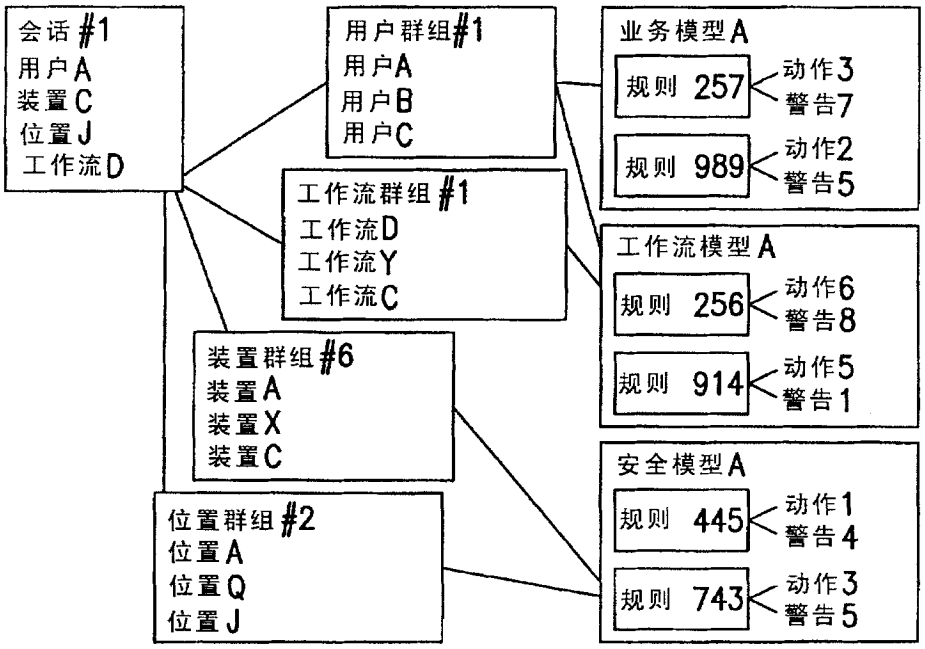

会话 #1
用户A
装置C
位置J
工作流D
用户群组#1
用户A
用户B
用户C
工作流群组 #1
工作流D
工作流Y
工作流C
装置群组 #6
装置A
装置X
装置C
位置群组 #2
位置A
位置Q
位置J
业务模型A
规则 257
动作3
警告7
规则 989
动作2
警告5
工作流模型A
规则 256
动作6
警告8
规则 914
动作5
警告1
安全模型A
规则 445
动作1
警告4
规则 743
动作3
警告5

图 16B

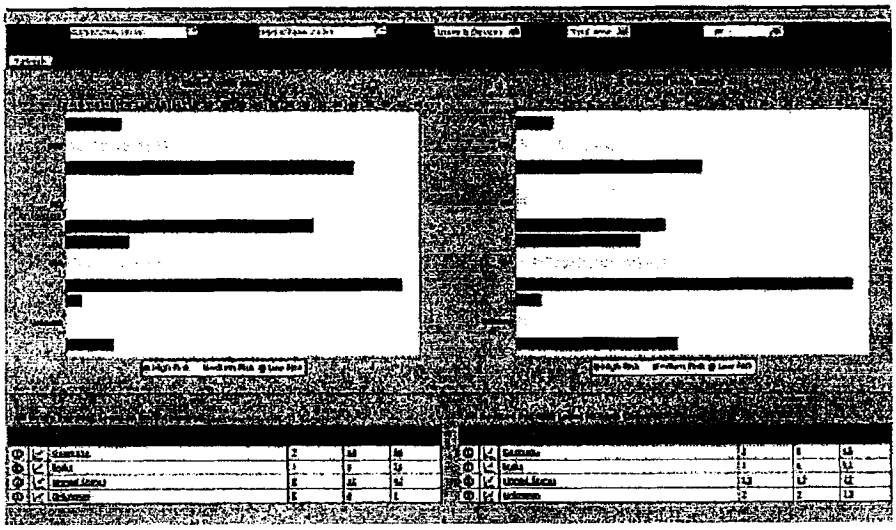


图 17A

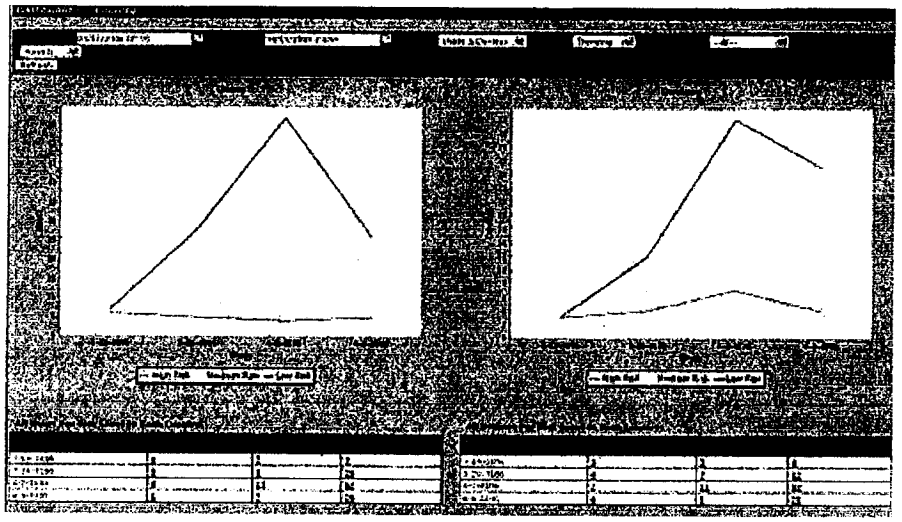


图 17B

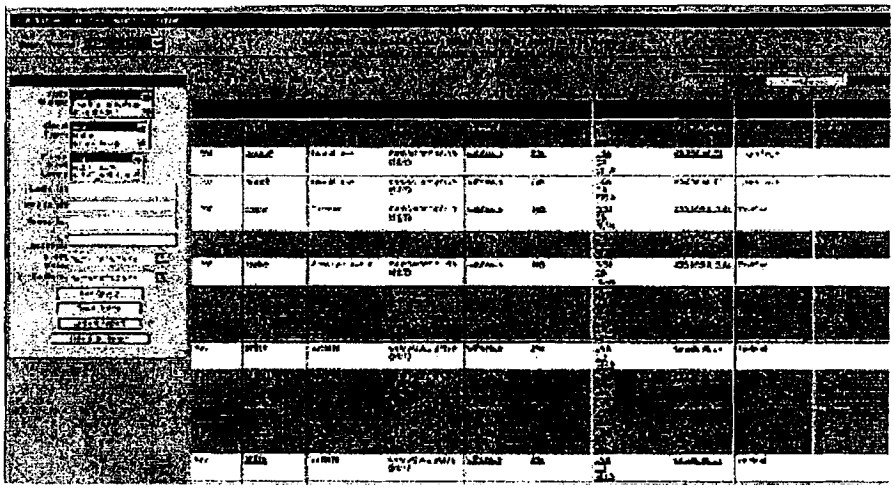


图 17C

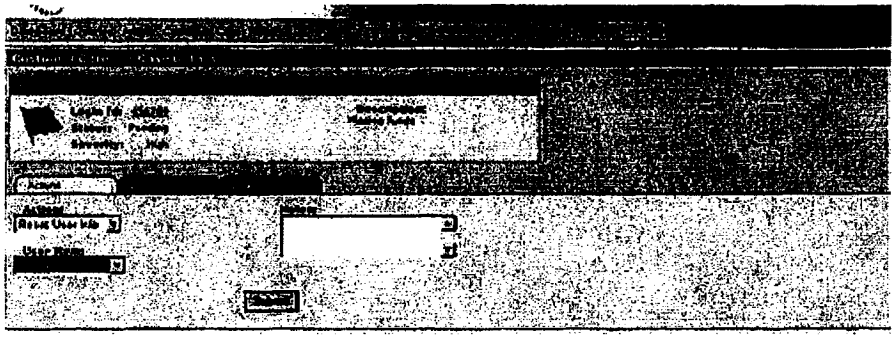


图 17D