



(12) 发明专利

(10) 授权公告号 CN 107925575 B

(45) 授权公告日 2021. 10. 26

(21) 申请号 201680045973.4

(22) 申请日 2016.06.10

(65) 同一申请的已公布的文献号
申请公布号 CN 107925575 A

(43) 申请公布日 2018.04.17

(30) 优先权数据
14/745826 2015.06.22 US

(85) PCT国际申请进入国家阶段日
2018.02.05

(86) PCT国际申请的申请数据
PCT/US2016/036807 2016.06.10

(87) PCT国际申请的公布数据
W02016/209637 EN 2016.12.29

(73) 专利权人 诺顿卫复客公司
地址 美国亚利桑那州

(72) 发明人 B·E·麦科肯德尔 W·E·曹贝乐

(74) 专利代理机构 中原信达知识产权代理有限
责任公司 11219

代理人 周亚荣 安翔

(51) Int.Cl.
H04L 9/12 (2006.01)
H04L 9/32 (2006.01)

(56) 对比文件
CN 101136906 A, 2008.03.05
CN 104243504 A, 2014.12.24
US 2014330918 A1, 2014.11.06
US 2006031301 A1, 2006.02.09
US 2010235877 A1, 2010.09.16
JohnMMeredith.Security aspects of
Machine-Type Communications (MTC) and
other mobile data applications
communications enhancements.《3GPP》.2013,
全文.

审查员 谭菲菲

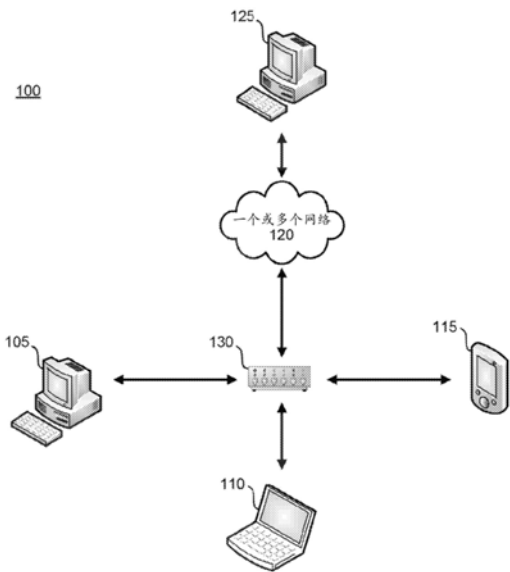
权利要求书2页 说明书14页 附图9页

(54) 发明名称

用于管理网络通信隐私的技术

(57) 摘要

本公开提供了用于管理网络通信隐私的技术,该技术可被意识到为计算机实现的系统,该系统包括存储指令的一个或多个处理器,以及执行指令进行以下操作的一个或多个计算机处理器:接收第一网络通信,从第一网络通信提取信息,基于信息识别隐私规则,基于第一网络通信和隐私规则生成第二网络通信并且致使第二网络通信被发送。



1. 一种用于管理网络通信隐私的计算机实现的系统,所述系统包括:
存储指令的一个或多个存储器设备;以及
适用于以下操作的一个或多个计算机处理器:
接收第一网络通信;
从所述第一网络通信中提取信息;
从多个隐私规则中识别隐私规则,其中所述隐私规则中的每一个隐私规则识别相关联的网络路由方案,并且其中,所述隐私规则至少部分地基于从多个路由器获得的集中的数据;
根据与所识别的所述隐私规则相关联的所述网络路由方案生成包括所述第一网络通信的第二网络通信;以及
致使所述第二网络通信被发送。
2. 根据权利要求1所述的系统,其中所述第二网络通信包括来自所述第一网络通信的数据,并且所述系统包括适用于生成和发送所述第二网络通信的路由器。
3. 根据权利要求1所述的系统,其中所述系统还包括存储设备,并且所述多个隐私规则存储在所述存储设备上。
4. 根据权利要求1所述的系统,其中,所述隐私规则还部分基于从所述第一网络通信中提取的所述信息的类别以及与客户端设备相关联的位置。
5. 根据权利要求4所述的系统,其中所述一个或多个处理器还执行所述指令以:
识别与域名或IP地址相关联的网站类别;以及
基于所述网站类别识别所述隐私规则。
6. 根据权利要求1所述的系统,其中基于与客户端设备在发送所述第一网络通信中所使用的一个或多个端口或协议相关的所述信息来识别所述隐私规则。
7. 根据权利要求1所述的系统,其中所述隐私规则由客户端设备的用户进行配置。
8. 根据权利要求1所述的系统,其中所述信息指示客户端设备的用户想要匿名化所述第二网络通信。
9. 根据权利要求1所述的系统,其中通过将来自所述第一网络通信的一个或多个消息封装在一个或多个加密层中来生成所述第二网络通信。
10. 根据权利要求9所述的系统,其中所述第二网络通信被生成用于在洋葱路由网络上发送。
11. 根据权利要求1所述的系统,其中所述第二网络通信被生成用于在虚拟专用网络(VPN)上发送。
12. 一种用于管理网络通信隐私的计算机实现的方法,所述方法包括:
从客户端设备接收第一网络通信;
从所述第一网络通信中提取信息;
通过一个或多个计算机处理器从多个隐私规则中识别隐私规则,其中所述隐私规则中的每一个隐私规则识别相关联的路由方案,并且其中,所述隐私规则至少部分地基于从多个路由器获得的集中的数据;
基于根据与所识别的所述隐私规则相关联的所述路由方案从所述第一网络通信生成第二网络通信;以及

发送所述第二网络通信。

13. 根据权利要求12所述的方法, 其中, 所述隐私规则还部分基于从所述第一网络通信中提取的所述信息的类别以及与客户端设备相关联的位置。

14. 根据权利要求13所述的方法, 还包括:

识别与域名或IP地址相关联的网站类别; 并且

基于所述网站的类别识别所述隐私规则。

15. 根据权利要求12所述的方法, 其中基于与所述客户端设备在发送所述第一网络通信中所使用的一个或多个端口或协议相关的所述信息来识别所述隐私规则。

16. 根据权利要求12所述的方法, 其中所述隐私规则由所述客户端设备的用户进行配置。

17. 根据权利要求16所述的方法, 其中所述信息指示所述客户端设备的所述用户想要匿名化所述第二网络通信。

18. 根据权利要求12所述的方法, 其中通过将来自所述第一网络通信的一个或多个消息封装在一个或多个加密层中来生成所述第二网络通信。

19. 根据权利要求12所述的方法, 其中所述第二网络通信包括来自所述第一网络通信的数据, 还包括通过生成并发送所述第二网络通信来路由所述第一网络通信。

20. 存储指令的非暂态计算机可读介质, 当由一个或多个计算机处理器执行时, 所述指令致使所述一个或多个计算机处理器执行用于管理网络通信隐私的方法, 所述方法包括:

接收第一网络通信;

从所述第一网络通信中提取信息;

从多个隐私规则中识别隐私规则, 其中所述隐私规则中的每一个隐私规则识别相关联的网络路由方案, 并且其中, 所述隐私规则至少部分地基于从多个路由器获得的集中的数据;

根据与所识别的所述隐私规则相关联的所述路由方案从所述第一网络通信生成第二网络通信; 以及

发送所述第二网络通信。

用于管理网络通信隐私的技术

[0001] 相关专利申请的交叉引用

[0002] 本专利申请要求于2015年6月22日提交的美国非临时专利申请14/745,826的优先权,该专利申请全文以引用方式并入本文。

技术领域

[0003] 本公开涉及网络通信技术,并且更具体地讲涉及用于管理网络通信隐私的技术。

背景技术

[0004] 这些年来,使用电子设备访问网络上的内容有了显著增长。如今,人们通过访问诸如互联网的网络上的网站来获取信息,分享他们的观点,管理他们的个人生活,娱乐以及出于其他许多原因。由于当今人们的大部分日常生活都涉及“在线”通信,因此监视或拦截这些通信的实体诸如公司、黑客、政府等可获得大量信息。此外,这些实体中的许多实体出于个人收益、销售或控制权而被激励去收集这些信息。例如,一些公司可能会将这些信息出售给其他公司,这些公司可将这些信息用于向具有某些特征的人群投放目标广告。又如,专制政府可使用这些信息来识别不同意他们政策的人或企图组织抗议活动的人。然而,个人可能不希望他们的通信能够被这些实体访问。具体地讲,为了避免被监视或拦截,个人可能不愿意在线提供某些个人信息,诸如关于他们的金融或政治思想的信息。

[0005] 已经使用了不同的技术来保护、加密并且/或者匿名化通信。然而,这些技术可能是有限制的、实现起来太复杂和/或不方便的。这些技术对于网络通信可能也具有一些缺点,诸如增加的数据包大小和较慢的网络通信速度。此外,许多用户甚至可能不知道可以使用这些技术。

[0006] 鉴于上述,可以理解,可能存在与当前网路通信技术相关联的显著问题和缺陷。

发明内容

[0007] 公开了用于管理网络通信隐私的技术。此外,本公开提供了基于一个或多个规则加密并且/或者匿名化网络通信。

[0008] 根据本公开,提供了用于管理网络通信隐私的计算机实现的系统。该系统包括存储指令的一个或多个存储器设备以及执行指令的一个或多个计算机处理器。该一个或多个计算机处理器执行指令以接收第一网络通信,并且从第一网络通信中提取信息。该一个或多个计算机处理器执行指令以基于该信息识别隐私规则。该一个或多个计算机处理器执行指令以基于第一网络通信和隐私规则生成第二网络通信,并且致使第二网络通信被发送。

[0009] 根据本公开的其他方面,第二网络通信包括来自第一网络通信的数据,并且该系统是通过生成并发送第二网络通信来路由第一网络通信的路由器。

[0010] 根据本公开的附加方面,该系统还包括存储设备,并且隐私规则是从存储在存储设备上的多个隐私规则中选择出来的。

[0011] 根据本公开的另一个方面,基于与特定域名或因特网协议(IP)地址相关的信息来

识别隐私规则。

[0012] 根据本公开的其他方面,一个或多个处理器还执行指令以识别与域名或IP地址相关联的网站的类别,并且基于网站的类别识别隐私规则。

[0013] 根据本公开的其他方面,基于与客户端设备在发送第一网络通信中所使用的一个或多个端口或协议相关的信息来识别隐私规则。

[0014] 根据本公开的其他方面,隐私规则由客户端设备的用户进行配置。

[0015] 根据本公开的附加方面,该信息指示客户端设备的用户想要匿名化第二网络通信。

[0016] 根据本公开的另一个附加方面,通过将来自第一网络通信的一个或多个消息封装在一个或多个加密层中来生成第二网络通信。

[0017] 根据本公开的其他方面,第二网络通信被生成用于在洋葱路由网络上发送。

[0018] 根据本公开的附加方面,第二网络通信被生成用于在虚拟专用网络 (VPN) 上发送。

[0019] 此外,根据本公开,提供了用于管理网络通信隐私的计算机实现的方法。该方法包括从客户端设备接收第一网络通信,并且从第一网络通信中提取信息。该方法还包括通过一个或多个计算机处理器基于该信息识别隐私规则。该方法还包括基于隐私规则从第一网络通信生成第二网络通信,并发送第二网络通信。

[0020] 根据本公开的其他方面,基于与特定域名或因特网协议 (IP) 地址相关的信息来识别隐私规则。

[0021] 根据本公开的其他方面,该方法还包括识别与域名或IP地址相关联的网站的类别,并且基于网站的类别识别隐私规则。

[0022] 根据本公开的其他方面,基于与客户端设备在发送第一网络通信中所使用的一个或多个端口或协议相关的信息来识别的隐私规则。

[0023] 根据本公开的其他方面,隐私规则由客户端设备的用户进行配置。

[0024] 根据本公开的其他方面,该信息指示客户端设备的用户想要匿名化第二网络通信。

[0025] 根据本公开的其他方面,通过将来自第一网络通信的一个或多个消息封装在一个或多个加密层中来生成第二网络通信。

[0026] 根据本公开的其他方面,第二网络通信包括来自第一网络通信的数据,并且该方法还包括通过生成并发送第二网络通信来路由第一网络通信。

[0027] 另外,根据本公开,提供了存储指令的非暂态计算机可读介质,当由一个或多个计算机处理器执行时,该指令致使一个或多个计算机处理器执行用于管理网络通信隐私的方法。该方法包括接收第一网络通信,并且从第一网络通信中提取信息。该方法还包括基于该信息识别隐私规则。该方法还包括基于隐私规则从第一网络通信生成第二网络通信,并发送第二网络通信。

[0028] 现在将参考如附图所示的本公开的具体实施方案对本公开进行更详细的描述。虽然下文结合具体实施方案对本公开进行了描述,但应当理解,本公开并不限于此。可以使用本文教导内容的本领域的普通技术人员将认识到另外的具体实施、修改形式和实施方案,以及其他使用领域,这些在如本文所述的本公开的范围内,并且本公开相对于它们可具有显著实用性。

附图说明

[0029] 为了帮助理解本发明,现在参考附图,其中类似的标号表示类似的元件。这些附图不应被理解为限制本发明,而是旨在仅为示例性的。

[0030] 图1示出了用于实现与本公开一致的实施方案和特征的示例通信环境。

[0031] 图2示出了用于实现与本公开一致的实施方案和特征的另一个示例通信环境。

[0032] 图3示出了用于实现与本公开一致的实施方案和特征的又一个示例通信环境。

[0033] 图4示出了用于实现与本公开一致的实施方案和特征的另一个示例通信环境。

[0034] 图5示出了用于实现与本公开一致的实施方案和特征的示例计算环境的框图。

[0035] 图6示出了与本公开的实施方案一致的用于管理网络通信隐私的示例方法的流程图。

[0036] 图7示出了与本公开的实施方案一致的用于管理网络通信隐私的隐私配置文件的示例表。

[0037] 图8示出了与本公开的实施方案一致的用于管理网络通信隐私的web浏览器的示例屏幕。

[0038] 图9示出了用于实现与本公开一致的实施方案和特征的示例计算机系统的框图。

具体实施方式

[0039] 现在将详细参考本发明的示例实施方案,其中的某些示例在附图中示出。

[0040] 本公开的实施方案涉及用于管理网络通信隐私的计算机化系统、方法和媒介。本公开的实施方案包括用于基于一个或多个规则对网络通信进行加密并且/或者匿名化的计算机化系统、方法和媒介。

[0041] 这些年来,使用电子设备访问网络上的内容有了显著增长。如今,人们通过访问诸如互联网的网络上的网站来获取信息,分享他们的观点,管理他们的个人生活,娱乐以及出于其他许多原因。由于当今人们的大部分日常生活都涉及“在线”通信,因此监视或拦截这些通信的实体诸如公司、黑客、政府等可获得大量信息。此外,这些实体中的许多实体出于个人收益、销售或控制权而被激励去收集这些信息。例如,一些公司可能会将这些信息出售给其他公司,这些公司可将这些信息用于向具有某些特征的人群投放目标广告。又如,专制政府可使用这些信息来识别不同意他们政策的人或企图组织抗议活动的人。然而,个人可能不希望他们的通信能够被这些实体访问。具体地讲,为了避免被监视或拦截,个人可能不愿意在线提供某些个人信息,诸如关于他们的金融或政治思想的信息。

[0042] 图1示出了用于路由网络通信的示例通信环境100。在通信环境100中,路由器130可通过一个或多个网络120(诸如互联网)路由一个或多个计算设备105,110,115和一个或多个计算设备125之间的通信。计算设备105,110,115可通过局域网(LAN)连接到路由器130。当在互联网上与一个或多个计算设备125通信时,例如,通信可发生在数据包中。每个数据包可包括例如源地址字段、目的地址字段以及其他数据。例如,源地址字段和目的地址字段可包括因特网协议(IP)地址。当路由器130从计算设备105,110,115之一接收将在一个或多个网络120上进行通信的第一数据包时,它可将来自第一数据包的源IP地址和目的地IP地址保存在表中,并且可以在通过一个或多个网络120将第一数据包发送到计算设备125之前,将第一数据包的源地址字段中的源IP地址替换为路由器的IP地址。例如,当计算设备

105发送前往计算设备125的数据包时,路由器130可以将源IP地址(其可以是计算设备105的IP地址)保存在表中,并且可以在通过一个或多个网络120将该数据包发送到计算设备125之前,将第一数据包中的源IP地址替换为路由器的IP地址。

[0043] 当计算设备125接收到第一数据包时,其可以提取源IP地址。计算设备125然后通过发送第二数据包来传达回复。第二数据包可包括源地址字段、目的地址字段和其他数据。为了将第二数据包路由到发送第一数据包的计算设备(例如,计算设备105),可将第二数据包的目的地址字段设置为第一数据包的源地址(例如,路由器130的IP地址)。第二数据包的源地址字段可包括计算设备125的IP地址,当路由器130接收到第二数据包时,其可以识别出第二数据包的源地址是与第一数据包的目的地址相同的地址。基于该识别,路由器130可意识到第二数据包可能是对由计算设备105发送的第一数据包的响应,并且路由器可将第二数据包路由到计算设备105。

[0044] 当个人通过诸如互联网的网络进行通信时,这些通信可能会被诸如公司、黑客、政府等实体监视或拦截。因此,这些实体可访问它们拦截到的通信的源地址、目的地址和/或数据。但是,个人可能不希望他们通信的数据或他们的身份(例如,如源地址或目的地址所指示的那样)可由其他实体访问。

[0045] 可以使用不同的技术为网络通信添加隐私。这些技术中的一些技术可在路由器上实现,其可以在将通信路由到网络中的下一个目的地之前对通信进行加密并且/或者匿名化。

[0046] 图2示出了用于使用向网络通信添加隐私的一种技术的示例通信环境200。在通信环境200中,路由器130可通过一个或多个网络120(诸如互联网)路由一个或多个计算设备105,110,115和一个或多个计算设备125之间的通信。计算设备105,110,115可通过LAN连接到路由器130。与相对于图1所描述的示例类似,通信可发生在数据包中,并且每个数据包可包括例如源地址字段、目的地址字段以及其他数据。源地址字段和目的地址字段可包括例如IP地址。通信环境200还可包括一个或多个代理服务器235。虽然被示出为与一个或多个网络120分开,但是一个或多个代理服务器235可以是一个或多个网络120内的用于中继通信的计算设备。通信环境200中的通信可类似于相对于图1所描述的那样发生;然而,一个或多个代理服务器235可向通信添加附加的匿名水平。

[0047] 代理服务器235可以以与路由器130可操作的方式类似的方式进行操作(例如,如相对于图1所描述的那样)。当代理服务器235从路由器130接收到第一数据包时,它可将来自第一数据包的源IP地址(例如,路由器130的IP地址)和目的IP地址保存在表中,并且可以在通过一个或多个网络120将第一数据包发送到计算设备135之前,将第一数据包的源地址字段中的源IP地址替换为代理服务器235的IP地址。当计算设备125接收到第一数据包时,其可以提取源IP地址(例如,代理服务器235的IP地址)。计算设备125然后通过发送第二数据包来传达回复。第二数据包可包括源地址字段、目的地址字段和其他数据。为了将第二数据包路由到发送第一数据包的计算设备,可将第二数据包的目的地址字段设置为第一数据包的源地址(例如,代理服务器235的IP地址)。第二数据包的源地址字段可包括计算设备125的IP地址。

[0048] 当代理服务器235接收到第二数据包时,它可以识别出第二数据包的源地址是与第一数据包的目的地址相同的地址。基于该识别,代理服务器235可意识到第二数据包可能

是对由路由器130发送的第一数据包的响应,并且代理服务器可将第二数据包路由到路由器130。路由器130然后可将第二数据包路由到最初发送第一数据包的计算设备,如上文相对于图1所描述的那样。因此,通过向计算设备105,110,115和计算设备125之间的通信路径添加代理服务器为该通信添加了另一层匿名,因为在通信通过代理服务器235时,路由器130的身份(例如,IP地址)被替换为代理服务器235的身份(例如,IP地址)。这可被称为计算设备105,110,115和计算设备125之间的通信路径中的附加“跳跃”。虽然图2示出了涉及一个代理服务器的示例,但是计算设备105,110,115和计算设备125之间的通信可通过附加的代理服务器(附加跳跃)使通信进一步匿名化。

[0049] 图3示出了用于使用向网络通信添加隐私的另一种技术的示例通信环境300。在通信环境300中,路由器130可通过一个或多个网络120(诸如互联网)路由一个或多个计算设备105,110,115和一个或多个计算设备125之间的通信。计算设备105,110,115可通过LAN连接到路由器130。与相对于图1所描述的示例类似,通信可发生在数据包中,并且每个数据包可包括例如源地址字段、目的地址字段以及其他数据。源地址字段和目的地址字段可包括例如IP地址。通信环境300还可包括一个或多个虚拟专用网络(VPN)335。通信环境300中的通信可类似于相对于图1所描述的那样发生;然而,一个或多个VPN 335可向通信添加附加的匿名和/或安全水平。

[0050] VPN可通过公共网络(诸如互联网)扩展专用网络。它可以使计算设备能够在从专用网络的安全性和/或匿名性中受益的同时在公共网络上传达数据。可通过建立点对点连接来创建VPN,该点对点连接可通过一个或多个专用连接、虚拟隧道协议并且/或者使用加密来建立。安全VPN协议可包括例如互联网协议安全性(IPsec)、安全传输层协议(TLS)、安全套接层协议(SSL)、数据包传输层安全性协议(DTLS)、微软(Microsoft®)点对点加密术协议(MPPE)、微软(Microsoft®)安全套接字隧道协议(SSTP)、多路径虚拟专用网络协议(MPVN)、安全外壳(SSH)VPN协议以及其他协议。使用VPN加密通信并且/或者在可信网络上发送通信可能使实体更难以监视或拦截通信。例如,在实体可以理解通信中的信息之前,它们可能需要解密通信并且/或者绕过安全协议。

[0051] 图4示出了用于使用向网络通信添加隐私的又一种技术的示例通信环境400。在通信环境400中,路由器130可通过一个或多个诸如互联网的网络120(图4中未示出)路由一个或多个计算设备105,110,115(尽管在图4中仅示出了计算设备110)和一个或多个计算设备125之间的通信。计算设备105,110,115可通过LAN连接到路由器130。与相对于图1所描述的示例类似,通信可发生在数据包中,并且每个数据包可包括例如源地址字段、目的地址字段以及其他数据。源地址字段和目的地址字段可包括例如IP地址。通信环境400还可包括一个或多个洋葱路由器440至480。洋葱路由器440至480可以是与一个或多个网络120分开的计算设备,或者可以是一个或多个网络120内用于中继通信的计算设备。洋葱路由器440至480可以与一个或多个网络(未示出)连接在一起,使得洋葱路由器440至480中任何两个路由器之间都可以发生通信。

[0052] 在洋葱路由中,通信数据包可被封装在加密层中,类似于洋葱层。为了在洋葱路由网络上传输数据包,计算设备可从洋葱路由器列表中选择一组洋葱路由器。所选择的洋葱路由器列表然后可被布置到数据包将传输通过的通信路径中。图4示出了示例通信路径,其

中数据包通过洋葱路由器440、460和480被路由到计算设备125。

[0053] 可为通信路径中的每个洋葱路由器添加加密层,使得每个加密层可仅由通信路径中的一个对应的洋葱路由器解密。当数据包在通信路径中传递时,每个洋葱路由器可剥离一层加密层,仅显示数据包将被发送到的下一个目的地。因此,数据包的目的地可保持隐藏,直到通信路径中的最后一个洋葱路由器剥离最后一层加密层为止。此外,数据包的发送者可保持匿名,因为每个洋葱路由器只知道它从中接收数据包的洋葱路由器的源地址。因此,洋葱路由可以提供网络通信中的安全性和/或匿名性。

[0054] Tor是一种可以在洋葱路由网络上进行匿名通信的软件。个人可以安装(诸如Tor浏览器)的Tor软件,这可允许他们通过洋葱路由器的志愿者网络发送通信。当个人选择使用Tor发送通信时,包括数据包的目的地址的通信数据包可被多次加密并通过随机选择的洋葱路由器的通信路径发送。然后,每个洋葱路由器可以解密一个加密层,以仅显示通信路径中的下一个洋葱路由器。当通信路径中最后一个洋葱路由器解密最内层的加密层时,其可将通信数据包发送到它的最终目的地。

[0055] 上面讨论的技术仅仅是可用于向网络通信添加隐私的技术中的少数技术。然而,现有的用于向网络通信添加隐私的技术可能仅限于某些个人,实现起来太复杂并且可能不方便使用。而且,在向网络通信添加安全性和/或匿名性的同时,这些技术对于网络通信可能具有一些缺点。例如,由于数据包大小变更大以及处理时间(例如,由于解密引起的延迟)增加,使用加密可能会降低网络通信的速度。因此,即使个人理解如何向网络通信添加隐私,他们可能希望向不同类型的网络通信添加不同水平的隐私,以在不需要更高水平的隐私时获得更高的网络速度。然而,手动选择以在不同的网络通信技术之间进行转换对用户来说可能带来不便。

[0056] 本公开的实施方案可以解决与向网络通信添加隐私相关联的挑战。例如,本公开的实施方案提供了用于管理网络通信隐私的计算机化系统、方法和媒介。在一些实施方案中,计算机化系统、方法和媒介可基于一个或多个规则来加密并且/或者匿名化网络通信。例如,诸如路由器的计算设备可接收诸如通信数据包的第一网络通信,并且从第一网络通信中提取信息。该信息可涉及例如用户正在请求连接的IP地址或域名,或者涉及来自用户的将隐私水平添加到网络通信的请求。基于该信息,可识别隐私规则。然后可基于第一网络通信和隐私规则生成第二网络通信。例如,第二网络通信可以是被加密并且包括来自第一数据包的数据的第二数据包,和/或是包括来自第一数据包的数据但被重新路由到代理服务器的第二数据包。也就是说,第二网络通信可以是添加了一定水平的加密和/或匿名的第一网络通信的路由版本。第二网络通信然后可被发送到网络中前往该通信的最终目的地途中的下一个目的地。

[0057] 本文所公开的计算机实现的方法可例如由从一个或多个非暂态计算机可读介质接收指令的一个或多个计算机处理器执行。类似地,与本公开一致的系統可包括至少一个计算机处理器和存储器,并且存储器可以是非暂态计算机可读介质。

[0058] 如本文所用,非暂态计算机可读介质是指任何类型的物理存储器,可由计算机处理器读取的信息或数据可存储在这些存储器上。这些存储器的示例包括随机存取存储器(RAM)、只读存储器(ROM)、易失性存储器、非易失性存储器、硬盘驱动器、光盘ROM(CD ROM)、数字通用光盘(DVD)、闪存驱动器、磁条存储器、半导体存储器、光盘存储器、磁光盘存储器

和/或任何其他已知的物理存储介质。诸如“存储器”和“计算机可读存储介质”之类的单数术语还可指代多个结构,诸如多个存储器和/或多个计算机可读存储介质。

[0059] 如本文所用,除非另外指明,否则“存储器”可包括任何类型的计算机可读存储介质。计算机可读存储介质可存储由一个或多个处理器执行的指令,包括用于使一个或多个计算机处理器执行与本文所公开的实施方案一致的步骤或阶段的指令。另外,一个或多个计算机可读存储介质可用于实现计算机实现的方法。

[0060] 如本文所用,不定冠词“一个”和“一个”在包括连接词“包括”、“包括”和/或“具有”的开放式权利要求中表示“一个或多个”。

[0061] 图5是用于实现本公开的实施方案的示例计算环境500的框图。提供计算环境500中的部件的布置和数量是出于说明的目的。与本公开一致,可以进行附加的安排、部件数量的修改和其他修改。在一些实施方案中,计算环境500可对应于并且通过另一种方式表示相对于图1至图4所述的一个或多个通信环境中的任何一个通信环境。

[0062] 如图5所示,计算环境500可包括一个或多个客户端设备510、网络520,540,560、路由器530、中继器550和通信设备570。客户端设备510可通过一个或多个网络520,540,560耦接到一个或多个路由器530、中继器550和通信设备570。

[0063] 以举例的方式,客户端设备510可以是个人计算机、台式计算机、膝上型计算机、服务器、web服务器、移动计算机、移动电话、智能电话、平板电脑、上网本、电子阅读器、个人数字助理(PDA)、可穿戴计算机、智能手表、游戏设备、机顶盒、电视机、个人信息管理工具、便携式电子设备、智能家电、导航设备和/或其他类型的计算设备。在一些实施方案中,客户端设备510可包括相对于图1至图4所描述的客户端设备105,110,115之一。在一些实施方案中,客户端设备510可利用硬件设备和/或在其上运行的软件应用程序来实现。客户端设备510可通过一个或多个网络520,540,560与一个或多个计算机系统(例如,路由器530、中继器550、通信设备570)进行通信。客户端设备510可存储使得客户端设备510能够访问诸如互联网的网络上的资源的浏览器软件。在一些实施方案中,一个或多个客户端设备510可使用诸如图9的计算机系统900的计算机系统来实现。

[0064] 计算环境500可包括一个或多个网络520。在一个实施方案中,一个或多个网络520可以是一个或多个本地网络(例如,个人局域网(PAN)、LAN、城域网(MAN)),但是本公开并不限于此。一个或多个网络520可将客户端设备510与一个或多个路由器530、中继器550、通信设备570和/或其他客户端设备510连接。一个或多个网络520可包括一个或多个PAN、LAN、MAN、广域网(WAN)或这些网络的任何组合。一个或多个网络520可包括一个或多个各种不同网络类型的任意组合,包括以太网、内联网、双绞线、同轴电缆、光纤、蜂窝、卫星、电气与电子工程师协会(IEEE)802.11、Wi-Fi、地面站、互联网、红外线和/或其他类型的有线或无线网络。一个或多个网络520可包括具有用于实施向通信添加隐私的一种或多种技术(诸如相对于图1至图4所描述的一种或多种技术)的拓扑和功能的网络。

[0065] 一个或多个客户端设备510、中继器550和/或通信设备570可被配置为通过一个或多个网络520,540,560与一个或多个路由器530进行通信。路由器可以是可将消息中继到不同网络或网络的不同链路的家庭网关(HGW)中继器、网桥、交换机、接入点、集线器、连接点或任何其他类型的设备。在一些实施方案中,路由器可将数据(诸如加密数据和/或网络地址信息)附加到所接收的通信数据或从所接收的通信数据删除这些数据。路由器530可以是

用于中继网络消息的任何类型的设备,并且可以作为软件、硬件或者软件和硬件的组合存在。在一些实施方案中,路由器530可包括相对于图1至图4所描述的路由器130。在一些实施方案中,一个或多个路由器530可使用诸如图9的计算机系统900的计算机系统来实现。

[0066] 计算环境500还可包括一个或多个网络540。一个或多个网络540可将一个或多个中继器540与一个或多个路由器530和/或一个或多个通信设备570连接。一个或多个网络540可包括一个或多个PAN、LAN、MAN、WAN或这些网络的任何组合。一个或多个网络540可包括一个或多个各种不同网络类型的组合,包括以太网、内联网、双绞线、同轴电缆、光纤、蜂窝、卫星、IEEE 802.11、Wi-Fi、地面站、互联网和/或其他类型的有线或无线网络。一个或多个网络540可包括具有用于实施向通信添加隐私的一种或多种技术(诸如相对于图1至图4所描述的一种或多种技术)的拓扑和功能的网络。

[0067] 一个或多个客户端设备510、路由器530和/或通信设备570可被配置为通过一个或多个网络520,540,560与一个或多个中继器550进行通信。中继器550可以是可将消息中继到不同网络或网络的不同链路的路由器、网桥、网关、服务器、代理服务器、交换机或其他类型的设备。在一些实施方案中,中继器550可将数据(诸如加密数据和/或网络地址信息)附加到所接收的通信数据或从所接收的通信数据删除这些数据。路由器530可以是用于中继网络消息的任何类型的设备,并且可以作为软件、硬件或者软件和硬件的组合存在。在一些实施方案中,中继器550可包括相对于图1至图4所描述的代理服务器235或洋葱路由器(例如,洋葱路由器440至480之一)。在一些实施方案中,一个或多个路由器530可使用诸如图9的计算机系统900的计算机系统来实现。

[0068] 计算环境500还可包括一个或多个网络560。一个或多个网络560可将一个或多个通信设备570与一个或多个中继器550、路由器530和/或客户端设备510连接。一个或多个网络560可包括一个或多个PAN、LAN、MAN、WAN或这些网络的任何组合。一个或多个网络560可包括一个或多个各种不同网络类型的组合,包括以太网、内联网、双绞线、同轴电缆、光纤、蜂窝、卫星、IEEE 802.11、Wi-Fi、地面站、互联网和/或其他类型的有线或无线网络。一个或多个网络560可包括具有用于实施向通信添加隐私的一种或多种技术(诸如相对于图1至图4所描述的一种或多种技术)的拓扑⁷和功能的网络。

[0069] 一个或多个客户端设备510、路由器530和/或中继器550可被配置为与一个或多个通信设备570进行通信。通信设备570可包括可连接到一个或多个网络560并与客户端设备510进行通信的任何类型的计算设备。通信设备570可包括服务器、web服务器、服务器群、个人计算机、台式计算机、膝上型计算机、服务器、web服务器、移动计算机、移动电话、智能电话、平板电脑、上网本、电子阅读器、个人数字助理(PDA)、可穿戴计算机、智能手表、游戏设备、机顶盒、电视机、个人信息管理工具、便携式电子设备、智能家电、导航设备和/或其他类型的计算设备。在一些实施方案中,通信设备570可包括相对于图1至图4所描述的客户端设备125。在一些实施方案中,通信设备570可利用硬件设备和/或在其上运行的软件应用程序来实现。通信设备570可通过一个或多个网络520,540,560与一个或多个计算机系统(例如,一个或多个客户端设备510、路由器530、中继器550)进行通信。在一些实施方案中,一个或多个通信设备570可使用诸如图9的计算机系统900的计算机系统来实现。

[0070] 尽管图5的计算环境500示出了一个或多个分开的客户端设备510、路由器530、中继器550和通信设备570,但是本公开并不限于此。一个或多个路由器530、中继器550和/或

通信设备570中的任何一个可在同一计算机系统上一起实现,诸如在图9的计算机系统900上实现。

[0071] 尽管图5的计算环境500示出了一个或多个分开的网络520,540,560,但是本公开并不限于此。例如,本公开的实施方案可在仅利用一种或两种网络的计算环境中实现,该网络可以仅包括一个或多个本地网和/或广域网。

[0072] 图6示出了与本公开的实施方案一致的用于管理网络通信隐私的示例方法600的流程图。示例方法600可使用一个或多个计算机系统(例如,参见图9的计算机系统900)在计算环境中实现(例如,参见图5)。在一些实施方案中,方法600可由一个或多个路由器530、一个或多个中继器550或上述的任意组合来执行。

[0073] 在方法600的步骤602中,可接收第一网络通信。第一网络通信可从客户端设备(诸如客户端设备510)接收。第一网络通信可包括消息的一个或多个片段。例如,第一网络通信可包括由特定网络协议和/或网络协议层使用的一个或多个数据包、帧、数据报、单元或任何其他类型的消息片段。第一网络通信可以是旨在被路由到目的设备(诸如通信设备570)的通信。第一网络通信可包括信息。

[0074] 在方法600的步骤604中,可从网络通信中提取信息。该信息可识别例如客户端设备希望与之通信的特定通信设备的目的地址、域名或统一资源定位符(URL)。另选地或除此之外,该信息可识别客户端设备的一个或多个位置、客户端设备在发送网络通信中所使用的协议以及客户端设备在发送网络通信中所使用的端口的任意组合。另选地或除此之外,该信息可识别来自客户端设备的用户的将一定隐私水平添加到网络通信和/或添加到与该网络通信相关的其他网络通信的请求。

[0075] 在方法600的步骤606中,可基于该信息来识别隐私规则。例如,一个或多个隐私规则可存储在存储设备中。隐私规则可被存储为隐私配置文件,每个隐私配置文件可将用于匿名化并且/或者加密通信的一个或多个规则与一个或多个条件相关联。一个或多个条件可涉及可从网络通信提取的信息,使得可基于所提取的信息识别隐私配置文件。

[0076] 在方法600的步骤608中,可生成第二网络通信。在一些实施方案中,第二网络通信可包括来自第一网络通信的数据,并且可包括加密、不同的目的地址和/或用于向通信添加隐私的其他数据。在一些实施方案中,第二网络通信可以是第一网络通信的路由版本。也就是说,用于中继到目的设备(例如,通信设备570)的第一网络通信的消息信息可被包括在第二网络通信中。

[0077] 在方法600的步骤610中,可发送第二网络通信。例如,可将第二网络通信发送到客户端设备和目的通信设备之间的通信路径中的下一个中继器或路由器。

[0078] 图7示出了隐私配置文件的示例表,该表包括与它们相关联的条件和规则。例如,多个隐私配置文件可存储在路由器530和/或中继器550处的存储设备中。在一些实施方案中,条件可指定特定IP地址、URL或域名以及用于处理涉及特定IP地址、URL或域名的通信的一个或多个规则。例如,从第一通信中提取的信息可指示客户端设备正在请求访问web服务器并且/或者与web服务器交互,该web服务器与http://www.example.com相关联。可以为http://www.example.com指定条件,并且可以将一个或多个规则与该条件关联。当从第一网络通信提取的信息中识别出http://www.example.com时,实现方法600的计算机系统(例如,图9的计算机系统900)可知道将一个或多个规则应用于路由网络通信。

[0079] 在一些实施方案中,实现方法600的计算机系统(例如,图9的计算机系统900)可存储对网站进行分类的信息。可通过网络(例如,一个或多个网络520,540,560)从一个或多个服务器或提供此类信息的服务供应商接收该信息。该信息可在计算机系统的请求下接收或者定期接收。例如,该信息可指示<http://www.example.com>是一个金融网站。当从识别<http://www.example.com>的第一网络通信中提取出信息时,实现方法600的计算机系统(例如,图9的计算机系统900)可认识到<http://www.example.com>是一个金融网站,并且存在针对金融类网站的一个或多个隐私规则。在图7所示的示例中,当通信涉及与金融网站进行通信时,规则指示实现方法600的计算机系统(例如,图9的计算机系统900)应该使用通过VPN路由通信的加密。

[0080] 在一些实施方案中,隐私配置文件可与应用程序相关联。例如,如果从第一网络通信提取出的信息指示客户端设备正在使用约会应用程序的协议和/或端口进行通信,则可应用一个或多个规则来路由该通信。在图7所示的示例中,当信息指示客户端设备正在使用约会应用程序进行通信时,则可使用通过VPN发送通信的加密来路由该通信。

[0081] 在一些实施方案中,可使用客户端设备的位置来确定是否应用一个或多个隐私规则。例如,关于与各个位置相关联的风险因素的信息可存储在实现方法600的计算机系统(例如,图9的计算机系统900)中。在图7所示的示例中,当从第一网络通信提取出的信息指示客户端设备位于高风险位置(例如,具有专制政府的国家),并且还指示客户端设备正试图访问并且/或者与抗议活动网站交互时,规则可指示Tor应该用于在洋葱路由网络上路由通信。

[0082] 一个或多个条件和/或一个或多个规则的任何组合可用于隐私配置文件中。例如,隐私配置文件可包括与网站、网站类别、应用程序、应用程序类型、协议、端口、明确的用户隐私请求、网络活动类别、网络流量类别、客户端设备位置或任何其他条件相关的一个或多个条件的任意组合。隐私配置文件还可包括一个或多个规则的任意组合,诸如用于加密(例如,使用IPsec、TLS、SSL、DTLS、MPPE、SSTP、MPVPN、SSHVPN、洋葱路由以及Tor中的一个或多个)并且/或者匿名化(例如,使用代理服务器、洋葱路由和/或Tor)网络通信的规则。

[0083] 在一些实施方案中,客户端设备510可被配置为具有用于发出向通信添加隐私的明确请求的软件。该软件可包括例如用于web浏览软件的插件或任何其他类型的客户端应用程序。图8示出了具有在URL<http://www.example.com>上的示例网站上打开的网页的web浏览器的示例屏幕800。web浏览器包括插件软件,使得控制按钮(例如,按钮810)出现在浏览器中。虽然按钮810在屏幕800的右上方示出,但是按钮810可出现在浏览器软件的任何地方,诸如在任何工具栏、下拉菜单或其他图形用户界面元素中出现。用户可选择控制按钮来指示用户希望向网络通信添加隐私。

[0084] 在按下按钮之后,从客户端设备发出的或者作为浏览器应用程序的结果从客户端设备发出的所有网络通信都可使用先前描述的任何加密和/或匿名化技术来增加隐私水平。当用户不再希望向网络通信添加隐私时,他/她可再次按下控制按钮以禁止向网络通信添加隐私。在一些实施方案中,当按下控制按钮时,用户还可配置隐私水平以将其添加到通信。例如,用户可选择使用通过VPN、一定数量的代理跳跃、洋葱路由和/或Tor的某种类型的加密。当用户选择向网络通信添加隐私时,在方法600的步骤602中接收到的第一网络通信可包括指示明确的用户隐私请求的信息。然后,第二网络通信可以是在用户按下控制按钮

之后以及在用户再次按下控制按钮以禁止向网络通信添加隐私之前的任何一个或多个其他网络通信。

[0085] 条件和/或规则可通过明确的用户选择和/或服务供应商的选择被配置到隐私配置文件中。在一些实施方案中,条件和/或规则可由一个或多个学习算法的机器进行配置。例如,实现方法600的计算机系统(例如,图9的计算机系统900)可随时间推移学习哪些网站、网站类别、应用程序、应用程序类型、协议、端口、网络活动类别、网络流量类别、客户端设备位置或任何其他条件在用户选择(诸如使用控制按钮)向网络通信添加隐私之后经常涉及通信。因此,如果客户端设备的用户在访问与特定类型的尴尬音乐相关联的网站之前经常选择控制按钮,实现方法600的计算机系统(例如,图9的计算机系统900)可能学习到它应该自动向涉及这种网站的之后的网络通信添加隐私。类似地,实现方法600的计算机系统(例如,图9的计算机系统900)可学习客户端设备的用户在访问涉及任何一个或多个这些各种条件的内容时所选择应用的隐私规则的类型,并且可能学习到它应该自动向涉及相同条件组合的之后的网络通信添加该隐私水平。

[0086] 在一些实施方案中,服务供应商可将来自许多路由器530的机器学习的信息集中起来,并且在路由器530之间提供这些信息。例如,可以了解到,许多用户在访问<http://www.example.com>上的金融网站时经常选择向网络通信添加隐私。该信息可以被传送给其他路由器,使得当网络通信中的信息指示访问并且/或者与网站<http://www.example.com>交互的请求时,隐私被自动添加到网络通信中。

[0087] 尽管以上描述通常将实现方法600的计算机系统(例如,图9的计算机系统900)描述为自动将隐私添加到网络通信,但是可以认识到,计算机系统在执行附加隐私之前可以首先询问用户他/她是否希望向网络通信添加隐私。例如,如果计算机系统自动确定应将隐私添加到某些网络通信中,则它可向客户端设备发送指示建议将隐私添加到通信的消息。用户可选择指示他/她希望添加隐私的按钮或指示他/她不希望将添加隐私到网络通信的按钮。实现方法600的计算系统然后可基于用户的响应添加或者避免添加隐私加密和/或匿名化。

[0088] 图9是示出了可用于实现与本公开一致的实施方案的示例计算机系统900的框图,包括本文描述的示例系统和方法。计算机系统900可包括一个或多个计算设备910。计算机系统900可用于实现客户端设备510、路由器530、中继器550和/或通信设备570。提供计算机系统900中的部件的布置和数量是出于说明的目的。与本公开一致,可以进行附加的安排、部件数量的修改或其他修改。

[0089] 如图9所示,计算设备910可包括用于执行指令的一个或多个处理器920。以举例的方式,适用于执行指令的处理器可包括通用微处理器和专用微处理器两者以及任何类型的数字计算机的任何一个或多个处理器。计算设备910还可包括一个或多个输入/输出(I/O)设备930。以举例的方式,I/O设备930可包括按键、按钮、鼠标、操纵杆、触笔等。按键和/或按钮可以是物理的和/或虚拟的(例如,设置在触摸屏界面上)。计算设备910也可经由I/O 930连接到一个或多个显示器(未示出)。可使用一个或多个显示面板来实现显示器,该显示面板可包括例如一个或多个阴极射线管(CRT)显示器、液晶显示器(LCD)、等离子体显示器、发光二极管(LED)显示器、触摸屏式显示器、投影仪显示器(例如,投影在屏幕或表面上的图像、全息图像等)、有机发光二极管(OLED)显示器、场发射显示器(FED)、有源矩阵显示器、真

空荧光 (VFR) 显示器、三维 (3-D) 显示器、电子纸 (电子墨水) 显示器或上述类型的显示器的任何组合。

[0090] 计算设备910可包括一个或多个存储设备,该一个或多个存储设备被配置为存储由处理器920用于执行与所公开的实施方案一致的操作的数据和/或软件指令。例如,计算设备910可包括主存储器940,该主存储器被配置为存储一个或多个软件程序,当由一个或多个处理器920执行时,该软件程序致使一个或多个处理器920执行与所公开的实施方案一致的功能或操作。

[0091] 以举例的方式,主存储器940可包括NOR和/或NAND闪存设备、只读存储器 (ROM) 设备、随机存取存储器 (RAM) 设备等。计算设备910还可包括一个或多个存储介质950。以举例的方式,一个或多个存储介质950可包括硬盘驱动器、固态驱动器、磁带驱动器、独立磁盘 (RAID) 阵列的冗余阵列等。虽然图9仅示出了一个主存储器940和一个存储介质950,但是计算设备910可包括任何数量的主存储器940和存储介质950。此外,虽然图9示出了主存储器940和/或存储介质950作为计算设备910的一部分,但主存储器940和/或存储介质950可远程定位,并且计算设备910能够经由一个或多个网络520,540,560访问主存储器940和/或存储介质950。

[0092] 一个或多个存储介质950可被配置为存储数据,并且可存储从一个或多个客户端设备510、路由器530、中继器550和/或通信设备570接收的数据。该数据可采用或者表示各种内容或信息形式,诸如文档、表格、列表、IP地址、MAC地址、用户名、密码、认证信息、解密密钥或代码、客户端设备信息、安全信息、软件应用程序、文件以及任何其他类型的信息和/或可在网络应用程序中使用的内容或者它们的任何组合。在一些实施方案中,一个或多个存储介质950可被配置为存储网站分类信息、集中的隐私信息、路由表、隐私配置文件、隐私条件、隐私规则和/或用于实现本文所公开的实施方案的任何其他类型的信息。

[0093] 计算环境910还可包括一个或多个通信接口960。一个或多个通信接口960可允许软件和/或数据在一个或多个客户端设备510、路由器530、中继器550和/或通信设备570之间传输。通信接口960的示例可包括调制解调器、网络接口卡 (例如,以太网卡)、通信端口、个人电脑存储卡国际协会 (PCMCIA) 卡槽和卡、天线等。一个或多个通信接口960可将软件和/或数据以信号的形式传输,其可以是电信号、电磁信号、光信号和/或其他信号类型。信号可经由通信路径 (例如,一个或多个网络520,540,560) 被提供到一个或多个通信接口960或从一个或多个通信接口960提供,该通信路径可使用有线、无线、电缆、光纤、射频 (RF) 和/或其他通信信道实现。

[0094] 本文所公开的实施方案不限于被配置为执行专门任务的单独的程序或计算机。例如,路由器530或中继器550可包括计算设备910,该计算设备包括存储单个程序或多个程序的主存储器940,并且还可执行远离路由器530或中继器550定位的一个或多个程序。类似地,替代执行存储在这些设备上的程序或者除此之外,客户端设备510、路由器530、中继器550和/或通信设备570可执行一个或多个远程存储的程序。在一些示例中,路由器530和/或中继器550能够访问生成、保持和提供网络配置、安全、网站分类信息、隐私信息和/或其他信息的单独的服务器、路由器、中继器、网关和/或其他计算系统。

[0095] 本公开的实施方案可以解决与向网络通信添加隐私相关联的挑战。本文所公开的计算机化系统、方法和媒介可允许自动将隐私添加到与用户所关心的活动相关联的网络通

信,或者通过简单的按下按钮来添加隐私。此外,计算机化系统、方法和媒介可允许用户配置用于将隐私添加到网络通信的偏好并且/或者提供学习用户随时间推移向网络通信添加隐私的偏好。因此,可针对用户所担心的网络通信建立隐私配置文件,例如,隐私、身份盗窃、审查和/或被专制政府、组织或机构在线追踪的危险。隐私配置文件还可能与用户可能担心的尴尬的网络通信相关联,诸如与色情、性取向、恋物癖、约会或令人尴尬的音乐相关联的网络通信。因此,本文所公开的计算机化系统、方法和媒介提供了向不同通信添加不同隐私层的便捷方式,允许用户在网上自由表达自己,而不用担心不利后果。

[0096] 本文所述的主体可在数字电子电路中或者在计算机软件、固件或硬件中实现,包括在本说明书中公开的结构装置及其等同物或者它们的组合。本文所述的主体可被实现为一个或多个计算机程序产品,诸如有形地体现在信息载体(例如,在机器可读存储设备中)或体现在由一台计算机或多台计算机执行的传播信号中的一个或多个程序。计算机程序(也称为程序、软件、软件应用程序或代码)可以以任何形式的编程语言编写,包括编译语言或解释语言,并且其可以以任何形式进行部署,包括作为独立的程序或者作为适用于计算环境的模块、组件、子例程或其他单元。计算机程序不一定对应于文件。程序可存储在保存其他程序或数据的文件的一部分中,存储在专用于所考虑的程序的一个文件中或者存储在多个协调的文件中(例如,存储一个或多个模块、子程序或部分代码的文件)。计算机程序可部署一个站点的一台计算机或多台计算机上执行,或者分布在多个站点并通过通信网络互连。

[0097] 本说明书中描述的过程和逻辑流程(包括本文所述的主体方法步骤)可由执行一个或多个计算机程序的一个或多个可编程处理器执行,以通过对输入数据进行操作并且生成输出来执行本文所述的主体功能。该过程和逻辑流程也可由本文所述的主体的装置执行,并且可被实现为专用逻辑电路,例如,FPGA(现场可编程阵列)或ASIC(专用集成电路)。

[0098] 以举例的方式,适用于执行计算机程序的处理器可包括通用微处理器和专用微处理器两者以及任何类型的数字计算机的任何一个或多个处理器。通常,处理器可从只读存储器或随机存取存储器或两者接收指令和数据。

[0099] 基于本说明书的书面描述和方法的计算机程序在软件开发者的技能范围之内。各种程序或程序模块可使用各种编程技术来创建。例如,程序部分或程序模块可以用Java、C、C++、汇编语言或任何此类编程语言来设计。一个或多个此类软件部分或模块可被集成到计算机系统或现有的通信软件中。

[0100] 此时,应当注意,如上所示,根据如上所述的本公开管理网络通信的隐私添加可在一定程度上涉及输入数据的处理以及输出数据的生成。输入数据处理和输出数据生成可在硬件或软件中实现。例如,根据如上所述的本公开的专用集成电路或类似的或相关的电路中可采用特定的电子元件,以实现与管理网络通信的隐私添加相关联的功能。另选地,根据如上所述的本公开的根据指令操作的一个或多个计算机处理器可实现与管理网络通信的隐私添加相关联的功能。如果是这种情况,则其在本发明的范围之内,因为此类指令可存储在一个或多个非暂态计算机可读存储介质(例如,磁盘或其他存储介质)上,或经由加载到一个或多个载波中的一个或多个信号而传输到一个或多个计算机处理器。

[0101] 本公开并不限于本文所述的特定实施方案的范围。实际上,通过前述描述和附图,

除了本文所述的内容之外,本发明的其他各种实施方案和修改形式对于本领域的普通技术人员而言将是显而易见的。因此,此类其他实施方案和修改形式旨在落入本公开的范围。此外,虽然本文针对至少一个特定用途在至少一个特定环境中以至少一种特定具体实施的情形来对本公开进行了描述,但本领域的那些普通技术人员将认识到,本发明的适用性并不局限于此,并且本发明可针对任意数量的用途在任意数量的环境中有利地实施。因此,如下所述的权利要求应该根据本文所述的本公开的完整的广度和精神来理解,包括落入本公开的真实精神和范围内的所有系统、方法和非暂态计算机可读介质。

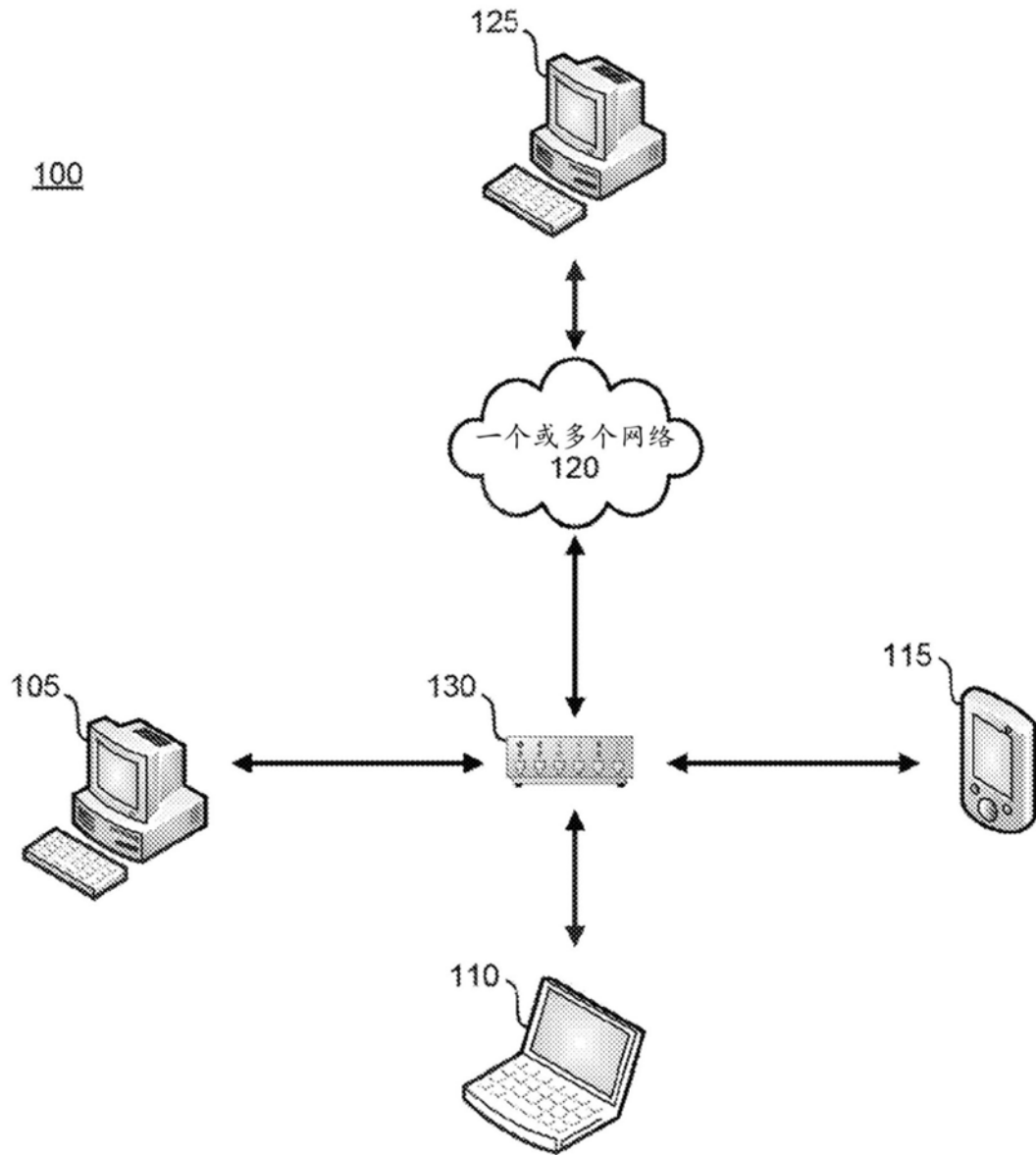


图1

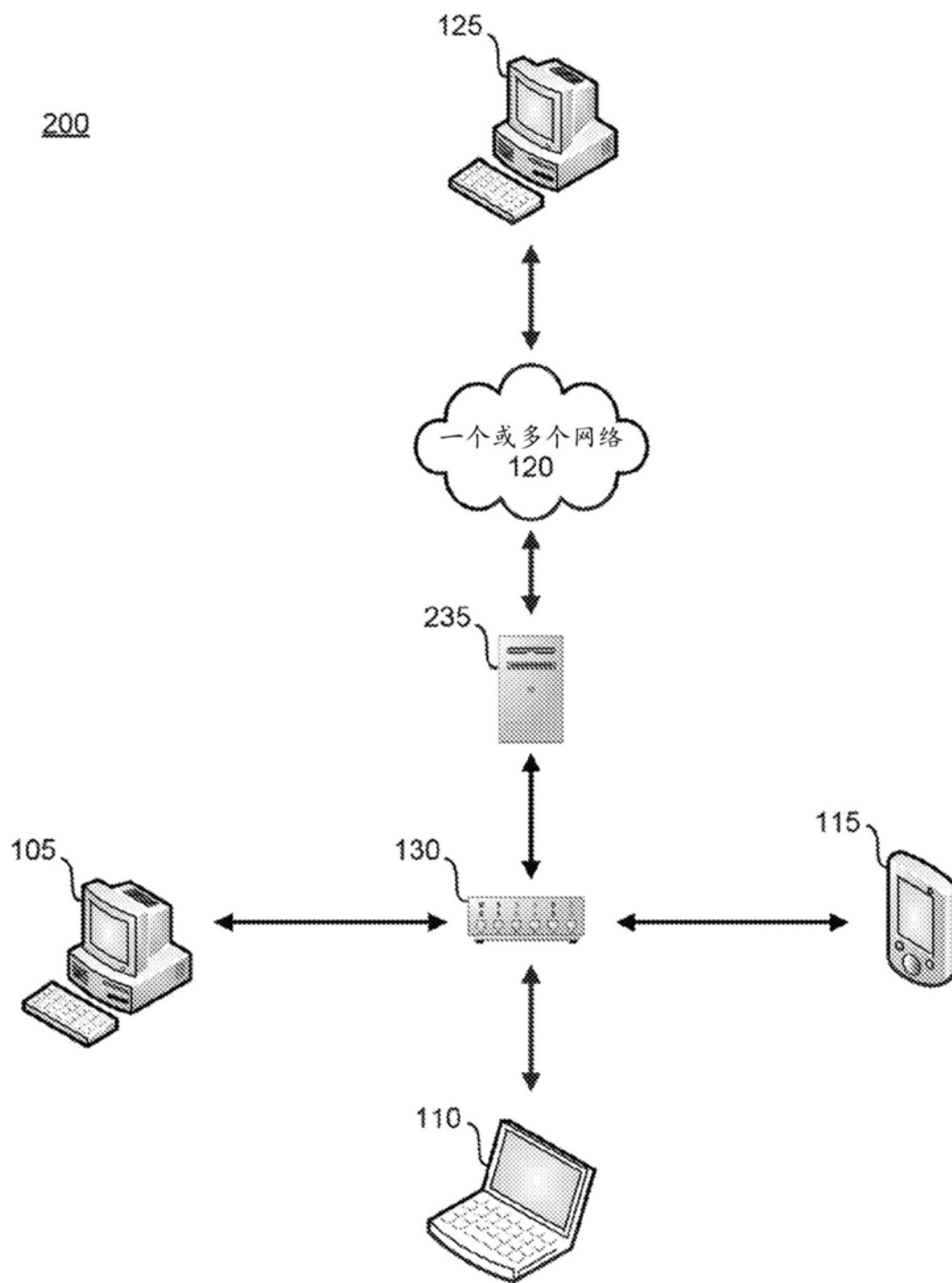


图2

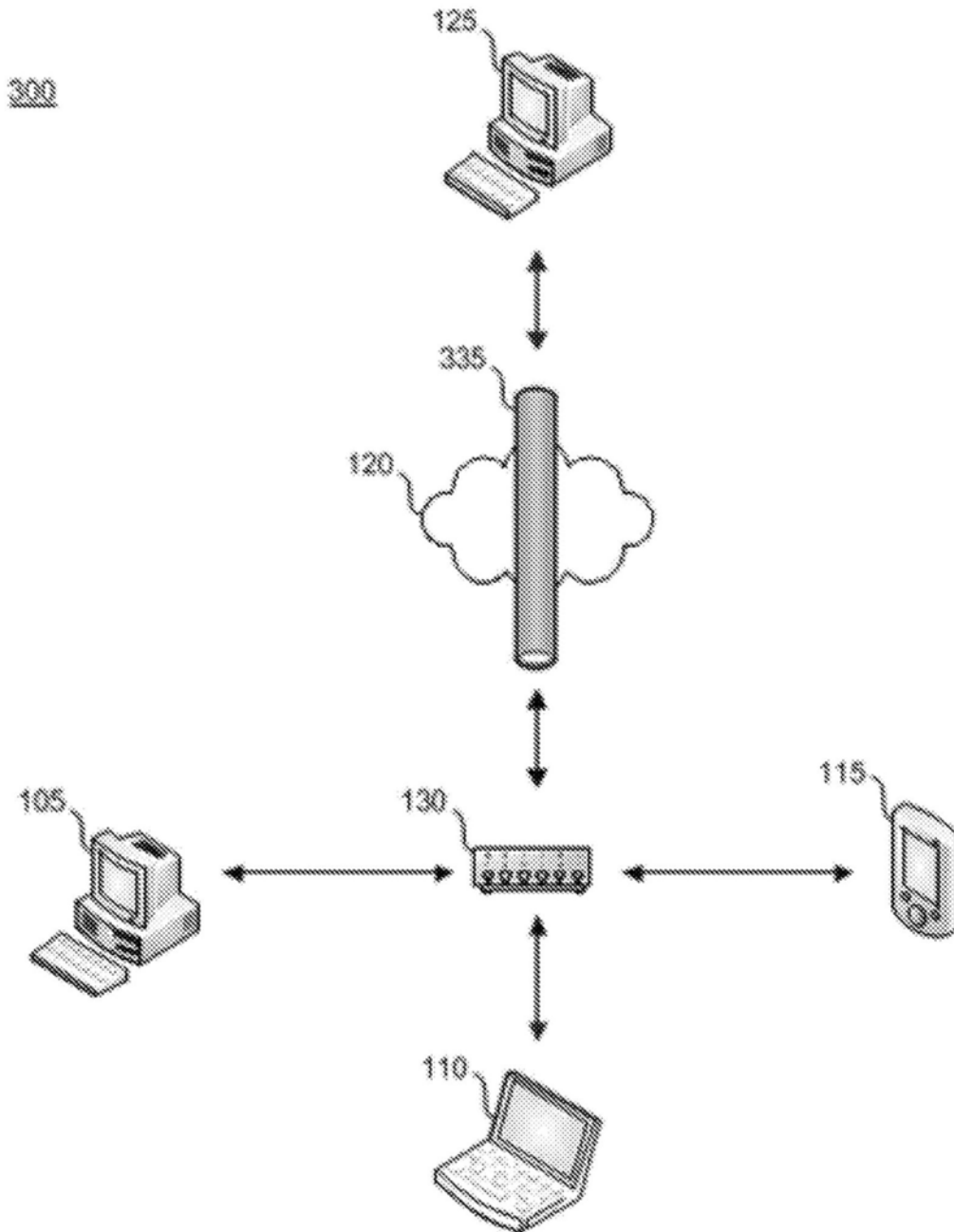


图3

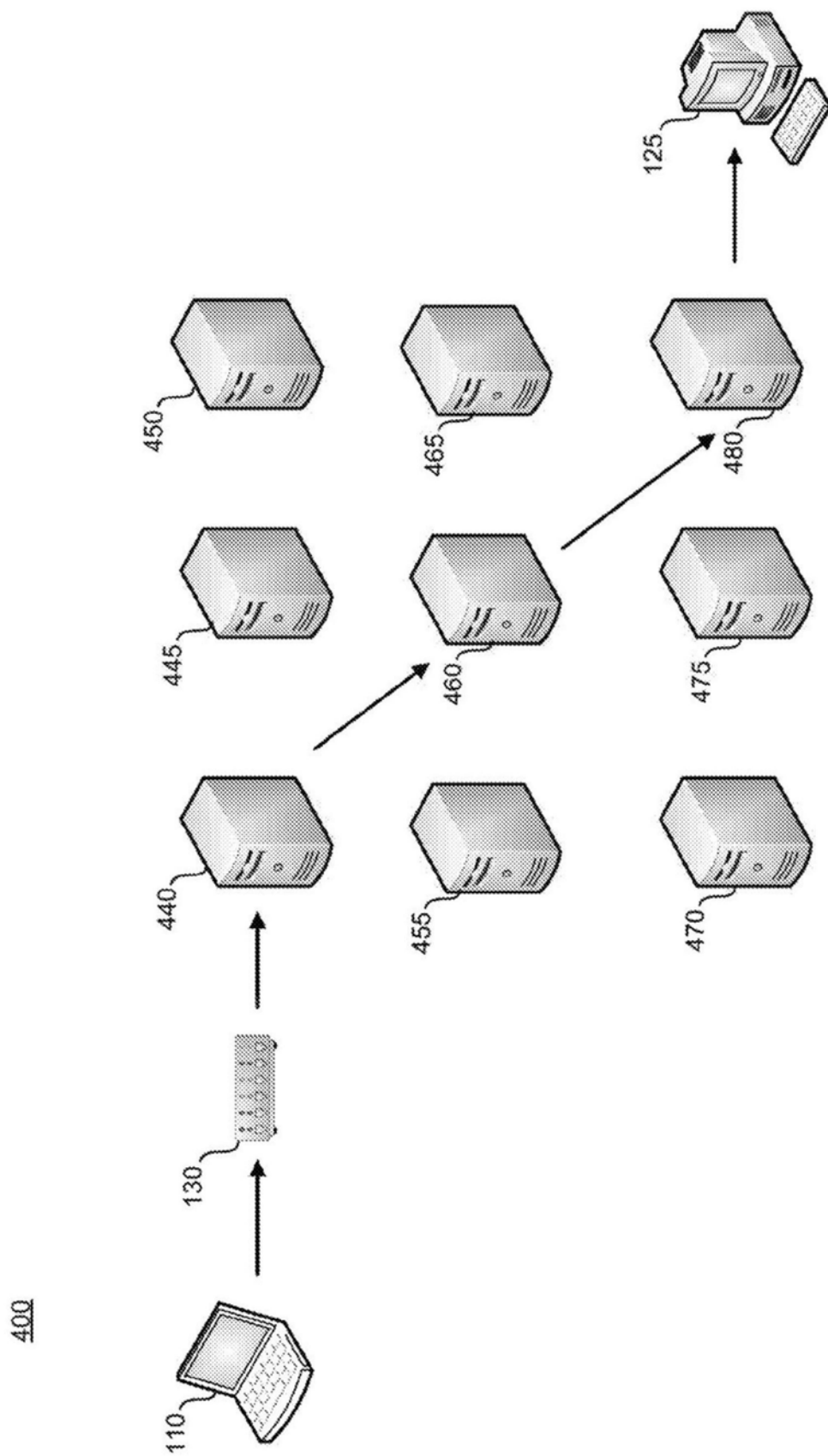


图4

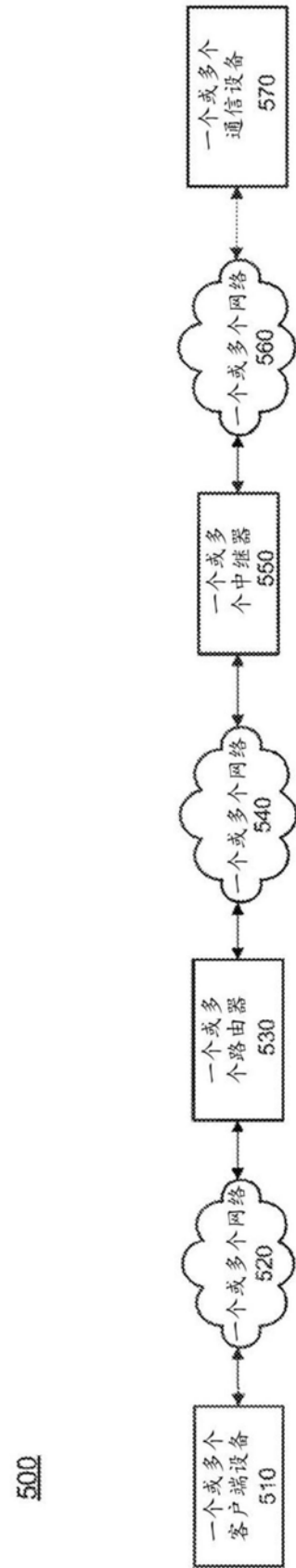


图5

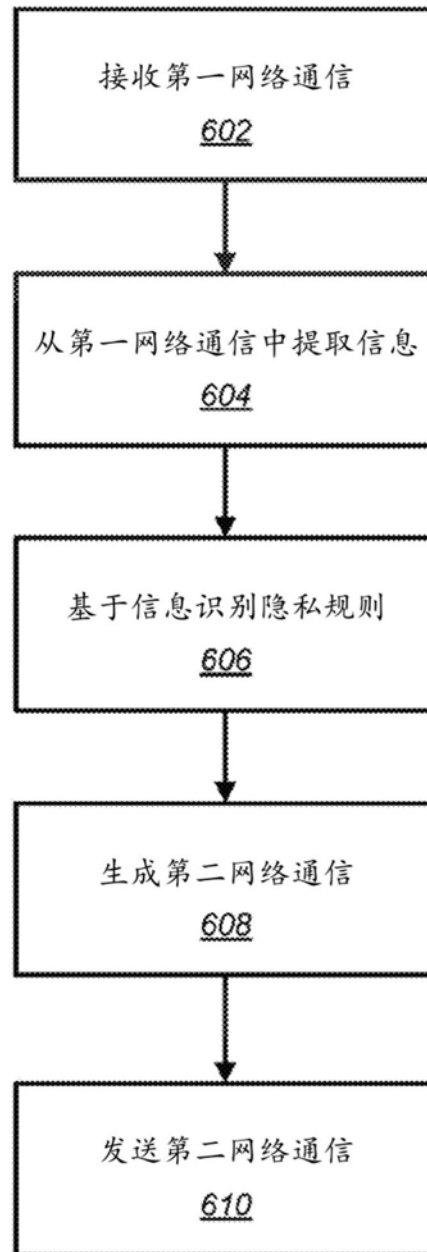
600

图6

700

条件	规则
金融网站	使用通过VPN发送的加密
抗议活动网站和高风险地点	使用通过洋葱路由发送的Tor
约会应用程序	使用通过VPN发送的加密
与尴尬的音乐相关的网站	经由至少两个代理服务器发送

图7

800

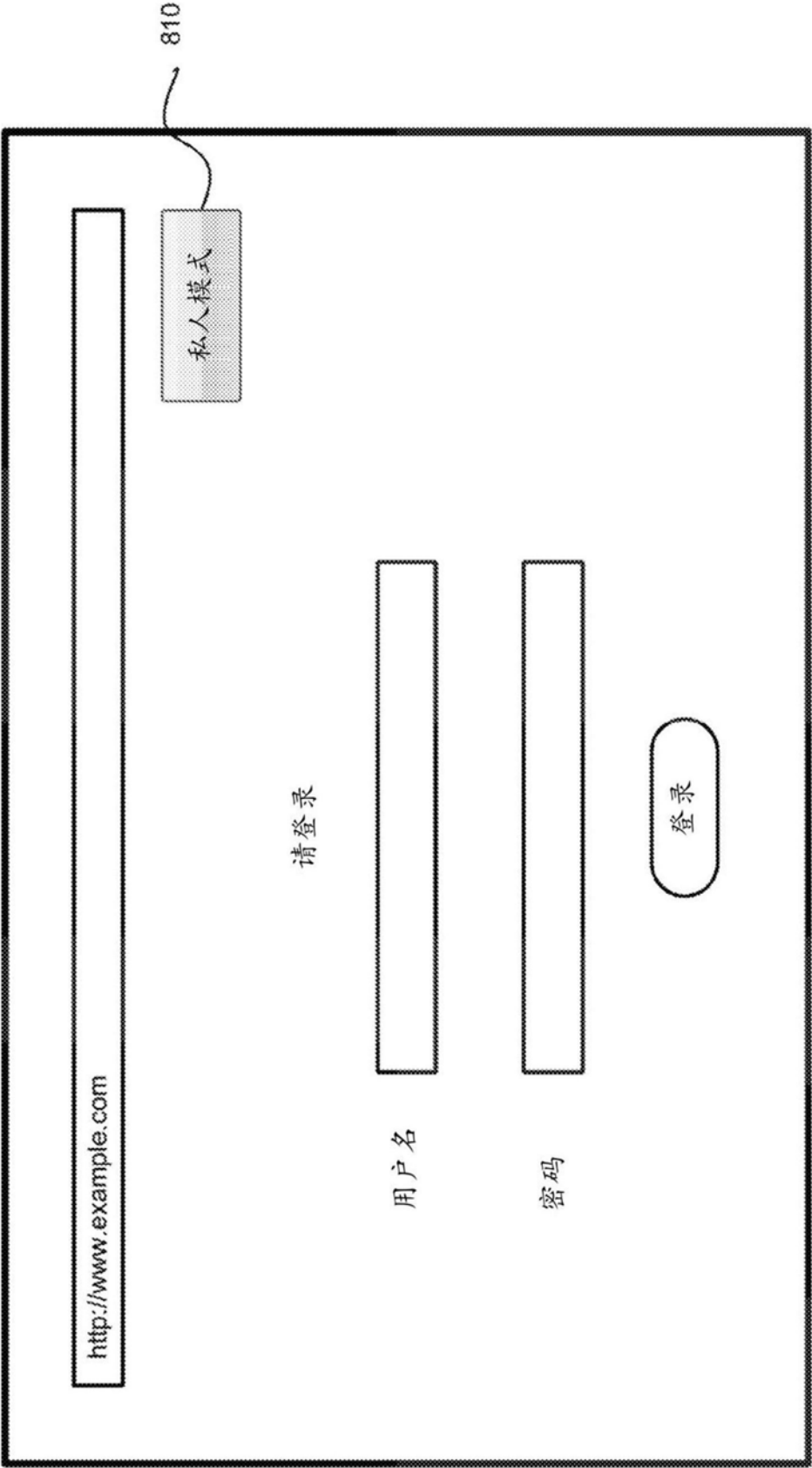


图8

900

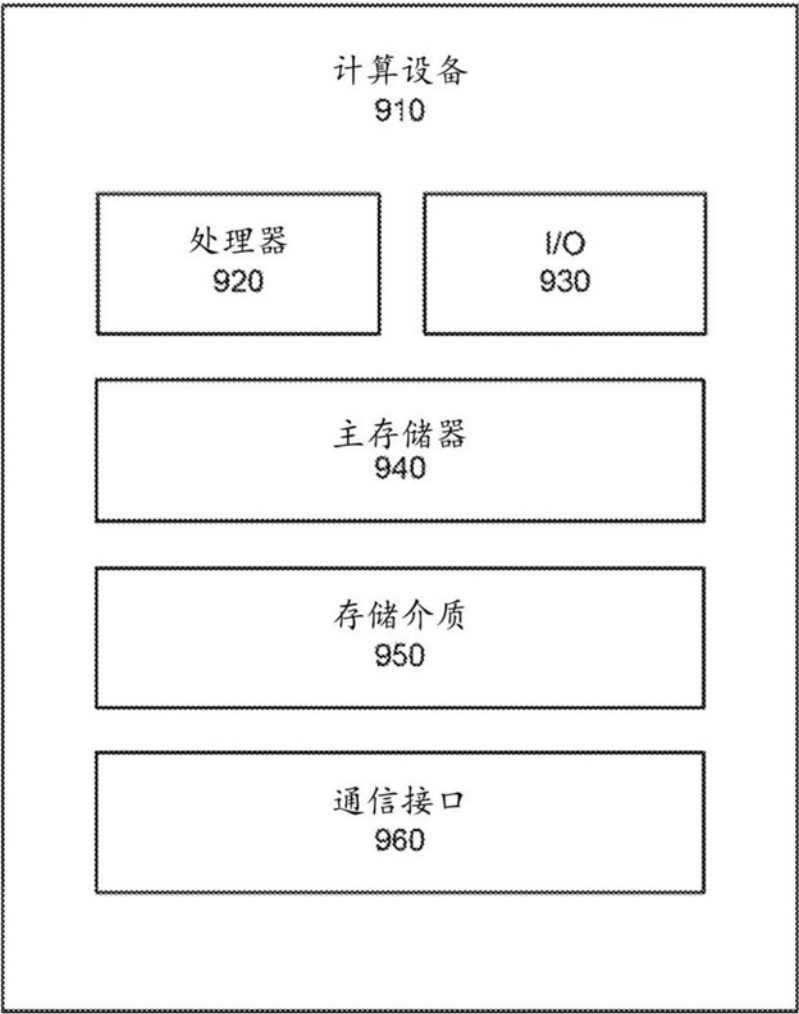


图9