(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112818392 A
(43)申请公布日 2021.05.18

(21)申请号 202110126653.4

(22)申请日 2021.01.29

(71)申请人 长沙市到家悠享网络科技有限公司
地址 410000 湖南省长沙市长沙高新开发区尖山路39号长沙中电软件园17栋401室

(72)发明人 胡海波

(74)专利代理机构 北京清诚知识产权代理有限公司 11691
代理人 宋红艳

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

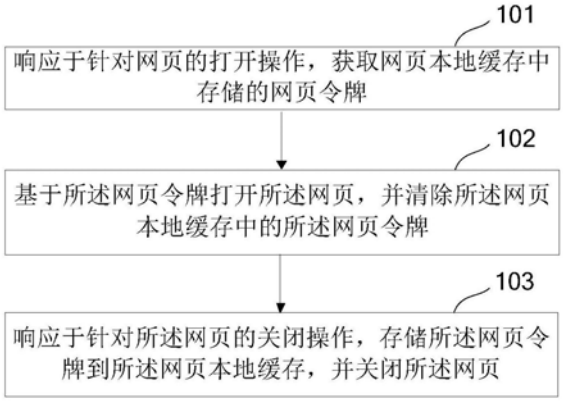
权利要求书2页 说明书8页 附图3页

(54)发明名称

网页安全处理方法、装置、设备和存储介质

(57)摘要

本发明公开了网页安全处理方法、装置、设备和存储介质。该方法包括:响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌;基于网页令牌打开网页,并清除网页本地缓存中的网页令牌;响应于针对所述网页的关闭操作,存储所述网页令牌到所述网页本地缓存,并关闭所述网页。通过上述方案,在打开网页的时候,为了避免网页令牌等相关安全信息被泄露,及时清除网页本地缓存中的网页令牌等相关安全信息,在网页关闭的时候,在将网页令牌等安全相关信息存储回网页本地缓存中,以便下次可以顺利打开网页,即便在网页打开期间,也无法从网页本地缓存中获取到网页令牌等相关安全信息,能够有效确保网页使用安全,确保用户个人信息安全。



CN 112818392 A

1.一种网页安全处理方法,其特征在于,应用于服务端,所述方法包括:

响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌;

基于所述网页令牌打开所述网页,并清除所述网页本地缓存中的所述网页令牌;

响应于针对所述网页的关闭操作,存储所述网页令牌到所述网页本地缓存,并关闭所述网页。

2.根据权利要求1所述的方法,其特征在于,响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌之前,还包括:

响应于针对网页的打开操作,判断所述网页令牌是否存储在系统全局变量中;

若所述系统全局变量中存储有所述网页令牌,则基于所述网页令牌打开所述网页。

3.根据权利要求2所述的方法,其特征在于,所述基于所述网页令牌打开所述网页,并清除所述网页本地缓存中的所述网页令牌,包括:

若所述系统全局变量中未存储所述网页令牌,则基于所述网页令牌打开所述网页;

存储所述网页令牌到所述系统全局变量中,并清除所述网页本地缓存中的所述网页令牌。

4.根据权利要求1所述的方法,其特征在于,响应于针对所述网页的关闭操作,存储所述网页令牌到所述网页本地缓存,并关闭所述网页之前,还包括:

响应于针对所述网页的关闭操作,判断所述网页令牌是否存储在系统全局变量中;

若所述系统全局变量中没有存储有所述网页令牌,则关闭所述网页。

5.根据权利要求4所述的方法,其特征在于,响应于针对所述网页的关闭操作,存储所述网页令牌到所述网页本地缓存,并关闭所述网页,包括:

响应于针对所述网页的关闭操作,判断所述网页令牌是否存储在所述系统全局变量中;

若所述系统全局变量中存储有所述网页令牌,则将所述网页令牌存储到所述网页本地缓存,关闭所述网页,并不清除所述系统全局变量中的网页令牌。

6.根据权利要求1至5中任一项所述的方法,其特征在于,所述网页本地存储为Localstorage,所述网页令牌为Token。

7.一种网页安全处理装置,其特征在于,应用于服务端,所述装置包括:

获取模块,用于响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌;

清除模块,用于基于所述网页令牌打开所述网页,并清除所述网页本地缓存中的所述网页令牌;

存储模块,用于响应于针对所述网页的关闭操作,存储所述网页令牌到所述网页本地缓存,并关闭所述网页。

8.一种电子设备,其特征在于,包括:处理器、存储器,所述存储器用于存储一条或多条计算机指令,其中,所述一条或多条计算机指令被所述处理器执行时实现权利要求1至6中任一项所述的网页安全处理方法。

9.一种存储有计算机程序的计算机可读存储介质,其特征在于,当所述计算机程序被一个或多个处理器执行时,致使所述一个或多个处理器执行包括以下的动作:

响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌;

基于所述网页令牌打开所述网页,并清除所述网页本地缓存中的所述网页令牌;

响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

网页安全处理方法、装置、设备和存储介质

技术领域

[0001] 本发明实施例涉及互联网技术领域，尤其涉及网页安全处理方法、装置、设备和存储介质。

背景技术

[0002] 随着互联网技术的发展，互联网普及到人们生活的方方面面。比如，登陆网上银行进行网上转账，登陆网上商城进行网上购物，进行家政服务预约等等。

[0003] 在实际业务应用中，用户在打开网页的时候，需要对用户的合法身份进行确认，比如Windows key或token。凡是拥有对应的Windows key就被认为是合法用户，进行相应登陆操作。Windows key能否妥善管理直接关系到用户个人信息的安全。若管理不善则会导致用户个人信息泄露，甚至会造成财产损失。

发明内容

[0004] 本发明实施例提供网页安全处理方法、设备和存储介质，用以提高基于用户实际需求进行会员套餐推广的技术方案。

[0005] 第一方面，本发明实施例提供一种网页安全处理方法，该方法包括：

[0006] 响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；

[0007] 基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；

[0008] 响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

[0009] 可选地，响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌之前，还包括：

[0010] 响应于针对网页的打开操作，判断所述网页令牌是否存储在系统全局变量中；

[0011] 若所述系统全局变量中存储有所述网页令牌，则基于所述网页令牌打开所述网页。

[0012] 可选地，所述基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌，包括：

[0013] 若所述系统全局变量中未存储所述网页令牌，则基于所述网页令牌打开所述网页；

[0014] 存储所述网页令牌到所述系统全局变量中，并清除所述网页本地缓存中的所述网页令牌。

[0015] 可选地，响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页之前，还包括：

[0016] 响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在系统全局变量中；

[0017] 若所述系统全局变量中没有存储有所述网页令牌，则关闭所述网页。

[0018] 可选地，响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页，包括：

[0019] 响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在所述系统全局变量中；

[0020] 若所述系统全局变量中存储有所述网页令牌，则将所述网页令牌存储到所述网页本地缓存，关闭所述网页，并不清除所述系统全局变量中的网页令牌。

[0021] 可选地，所述网页本地存储为Localstorage，所述网页令牌为Token。

[0022] 第二方面，本发明实施例提供一种网页安全处理装置，该装置包括：

[0023] 获取模块，用于响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；

[0024] 清除模块，用于基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；

[0025] 存储模块，用于响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

[0026] 第三方面，本发明实施例提供一种电子设备，包括处理器、存储器，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行时实现如第一方面所述的网页安全处理方法。

[0027] 第四方面，本发明实施例提供一种存储有计算机程序的计算机可读存储介质，当所述计算机程序被一个或多个处理器执行时，致使所述一个或多个处

[0028] 响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；

[0029] 基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；

[0030] 响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

[0031] 在本发明实施例中，响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。通过上述方案，在打开网页的时候，为了避免网页令牌等相关安全信息被泄露，及时清除网页本地缓存中的网页令牌等相关安全信息，在网页关闭的时候，在将网页令牌等安全相关信息存储回网页本地缓存中，以便下次可以顺利打开网页，即便在网页打开期间，也无法从网页本地缓存中获取到网页令牌等相关安全信息，能够有效确保网页使用安全，确保用户个人信息安全。

附图说明

[0032] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1为本申请实施例提供的一种网页安全处理方法的流程示意图；

[0034] 图2a为本申请实施例举例说明的网页打开的流程示意图；

[0035] 图2b为本申请实施例举例说明的网页关闭的流程示意图；

[0036] 图3为本申请实施例提供的一种网页安全处理装置的结构示意图；

[0037] 图4为与图3所述实施例提供的一种网页安全处理装置对应的电子设备的结构示意图。

具体实施方式

[0038] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0039] 在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义，“多种”一般包含至少两种。

[0040] 应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0041] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的商品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种商品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的商品或者系统中还存在另外的相同要素。

[0042] 随着互联网技术普及，互联网普及到人们生活的方方面面。比如，登陆网上银行进行网上转账，登陆网上商城进行网上购物，进行家政服务预约等等。用户在使用过程中，需要通过用户的token才能打开对应的网页。而这些token等相关安全信息通常直接存储到网页本地缓存local storage或cookie中，在用户浏览网页的同时，不法人员也可以很容易的获取到local storage中的token等相关安全信息。若token等相关安全信息被窃取，则可以利用token随意登陆网页，并进一步获取用户的更多秘密信息。因此，需要一种简单的实现用户安全浏览网页的技术方案。

[0043] 需要说明的是，本申请虽然举例说明的时候是为了实现对token、Windows key等进行安全防护，实际应用中还可以对其他任何用户想要保护的隐秘信息采用相同的技术方案达到安全防护的效果。这里仅作为举例说明，并不构成对本申请技术方案的限制。

[0044] 图1为本申请实施例提供的一种网页安全处理方法的流程示意图，应用于服务端(比如，云服务器或者服务器集群)，也可以应用于本地计算机，如图1所示，该方法包括以下步骤：

[0045] 101：响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌。

[0046] 102：基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌。

[0047] 103：响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

[0048] 在实际应用中,若用户打开想要操作的网页,则需要进行权限验证,通常是通过Windows key(比如token)进行验证,若验证通过,则允许用户继续通过网页进行相关操作。而Windows key通常会存储在local storage或者cookie中,在进行网页操作的时候,很容易被非法窃取。一旦Windows key被窃取,则表示任何拥有Windows key的人员随时可以冒充身份进行登陆网页以及基于网页的进一步操作,从而获取用户更多的隐秘信息。可见,将需要保密的信息数据存储在local storage或cookie中是比较危险的行为。

[0049] 这里所说的网页本地缓存可以是local storage或cookie等,这里所说的网页令牌可以是Windows key、token等。

[0050] 为了确保网页本地缓存中的网页令牌等相关安全信息的安全存储,在打开网页之后,需要对网页本地缓存中的网页令牌等相关安全信息进行清除。也就是,用户可以继续正常使用当前网页,即便个别网页想要通过非法途径获取网页本地存储中的信息,也是空白状态,或者获取到一些不是很重要的信息。

[0051] 当用户关闭网页的时候,还需要将之前被清除的网页令牌等相关安全信息重新写入到网页本地缓存当中。以便用户下一次打开网页的时候可以顺利通过Windows key验证并打开网页。

[0052] 通过上述方案,可以在打开网页之后对网页本地缓存中的Windows key等安全相关信息进行清除,在关闭网页的时候再将Windows key等安全相关信息写入到网页本地缓存中,既能确保用户在浏览网页的时候的信息安全防护效果,又能够不对用户的使用操作产生不利影响。

[0053] 在本申请一个或者多个实施例中,响应于针对网页的打开操作,获取网页本地缓存中存储的网页令牌之前,还包括:响应于针对网页的打开操作,判断所述网页令牌是否存储在系统全局变量中;若所述系统全局变量中存储有所述网页令牌,则基于所述网页令牌打开所述网页。

[0054] 在本申请技术方案中,对网页本地缓存清除之前,需要将网页本地缓存中需要被清除的信息复制存储到系统全局变量当中。当然,除此之外,也可以将网页本地缓存中的任何需要保密的信息存储到系统全局变量等安全性较高的存储位置。

[0055] 在实际应用中,用户想要打开网页的时候,先判断当前的系统全局变量中是否存储有打开网页所需的网页令牌,若存在,则表示可以直接利用预先存储在网页本地缓存中的网页令牌打开所需网页,并对网页对应的网页本地缓存中的网页令牌等相关信息进行清除。由于系统全局变量中已经存储有所需的网页令牌,则在对网页本地缓存进行清除之前不需要再将被清除信息复制到系统全局变量中。容易理解的是,若网页令牌发生变化,或者用户又有新的信息需要采用同样的方式进行安全存储,则需要在对网页本地缓存进行清除之前,对新的网页令牌或者用户想要保密的信息进行复制并存储到系统全局变量等安全存储位置。

[0056] 在本申请一个或者多个实施例中,所述基于所述网页令牌打开所述网页,并清除所述网页本地缓存中的所述网页令牌,包括:若所述系统全局变量中未存储所述网页令牌,则基于所述网页令牌打开所述网页;存储所述网页令牌到所述系统全局变量中,并清除所述网页本地缓存中的所述网页令牌。

[0057] 在一些实际应用场景中,还可能因为是新增网页令牌或者因为某些原因导致系统

全局变量丢失，在打开网页的时候从系统全局变量中并没有找到所需的网页令牌，则需要重新进行网页安全处理。具体来说，需要在基于网页令牌对网页进行打开操作的时候，将存储在网页本地缓存中的网页令牌复制到系统全局变量中进行存储，进而将在网页本地缓存中已经被备份存储到系统全局变量中相同的网页令牌进行清除。在每次开启网页的时候，都对系统全局变量中存储的网页令牌等相关信息进行有效性验证，能够在提供网页令牌等保密信息安全防护的同时，还能够确保不会因此导致用户无法正常使用，通过上述验证过程能够及时发现问题并解决问题。

[0058] 在本申请一个或者多个实施例中，响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页之前，还包括：响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在系统全局变量中；若所述系统全局变量中没有存储有所述网页令牌，则关闭所述网页。

[0059] 在实际应用中，由于一些原因比如，从网页本地缓存中复制网页令牌复制失败，或者系统全局变量中数据损坏或丢失，导致无法从系统全局变量中获取到想要的网页令牌。当需要关闭网页的时候，则无法将系统全局变量中的网页令牌存储到网页本地缓存中，将直接关闭网页。从而能够有效避免因为系统全局变量中没有存储网页令牌无法关闭网页的问题出现。

[0060] 在本申请一个或者多个实施例中，响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页，包括：响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在所述系统全局变量中；若所述系统全局变量中存储有所述网页令牌，则将所述网页令牌存储到所述网页本地缓存，关闭所述网页，并不清除所述系统全局变量中的网页令牌。

[0061] 在实际应用中，若用户点击关闭网页，对系统全局变量中存储的内容进行判断。若系统全局变量中存储有网页令牌，则在网页关闭之前，需要将网页令牌复制存储到网页本地缓存当中，在复制存储完成后，关闭网页。需要说明的是，虽然系统全局变量中的网页令牌被复制到网页本地缓存中，但是，系统全局变量中的网页令牌等相关安全信息不能被清除。当然在实际应用中，若某些信息是变化的，比如，每次使用完成之后，在下次使用的时候都会产生新的数据信息，则在关闭网页的时候，可以对系统全局变量中在先存储的信息进行清除，以便下次存入新的信息。当然，也可以对系统全局变量中信息进行清除，当有新的信息需要存入的时候，可以直接替换掉旧的无效信息。

[0062] 在本申请一个或者多个实施例中，所述网页本地存储为Localstorage，所述网页令牌为Token。

[0063] 为了便于理解，下面结合附图对网页的打开和关闭过程分别进行举例说明。如图2a为本申请实施例举例说明的网页打开的流程示意图。图2b为本申请实施例举例说明的网页关闭的流程示意图。

[0064] 如图2a所示，在用户打开浏览器之后，进而打开用户需要的网页，会判断Windows key是否存储在系统全局变量中。若存在，则直接打开网页，此时Windows key相当于所需token。若不存在，则从缓存(比如，网页本地缓存localstorage、cookie等)中获取对应的Windows key并挂在Windows上，也就是存储到系统全局变量中。进而将缓存中的key进行清除。

[0065] 如图2b所示，当用户想要关闭浏览器网页的时候，系统监听到unload事件，则进一步判断系统全局变量中是否存储有Windows key，若没有存储，则直接关闭网页浏览器，若存储，则将Windows key存入到缓存local storage中。然后关闭网页浏览器。

[0066] 基于上述实施例，响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。通过上述方案，在打开网页的时候，为了避免网页令牌等相关安全信息被泄露，及时清除网页本地缓存中的网页令牌等相关安全信息，在网页关闭的时候，在将网页令牌等安全相关信息存储回网页本地缓存中，以便下次可以顺利打开网页，即便在网页打开期间，也无法从网页本地缓存中获取到网页令牌等相关安全信息，能够有效确保网页使用安全，确保用户个人信息安全。既能确保用户在浏览网页的时候的信息安全防护效果，又能够不对用户的使用操作产生不利影响。

[0067] 基于相同的思路，本申请实施例还提供一种网页安全处理装置，该装置的执行主体可以是服务司机的客户端。如图3为本申请实施例提供的一种网页安全处理装置的结构示意图。从图3中可以看到所述装置包括：

[0068] 获取模块31，用于响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌。

[0069] 清除模块32，用于基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌。

[0070] 存储模块33，用于响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。

[0071] 可选地，获取模块31，还用于响应于针对网页的打开操作，判断所述网页令牌是否存储在系统全局变量中；

[0072] 若所述系统全局变量中存储有所述网页令牌，则基于所述网页令牌打开所述网页。

[0073] 可选地，清除模块32，用于若所述系统全局变量中未存储所述网页令牌，则基于所述网页令牌打开所述网页；

[0074] 存储所述网页令牌到所述系统全局变量中，并清除所述网页本地缓存中的所述网页令牌。

[0075] 可选地，存储模块33，用于响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在系统全局变量中；

[0076] 若所述系统全局变量中没有存储有所述网页令牌，则关闭所述网页。

[0077] 可选地，存储模块33，用于响应于针对所述网页的关闭操作，判断所述网页令牌是否存储在所述系统全局变量中；

[0078] 若所述系统全局变量中存储有所述网页令牌，则将所述网页令牌存储到所述网页本地缓存，关闭所述网页，并不清除所述系统全局变量中的网页令牌。

[0079] 可选地，所述网页本地存储为Local storage，所述网页令牌为Token。

[0080] 在一个可能的设计中，上述图3所示网页安全处理装置的结构可实现为一电子设备，如图4所示为与图3所述实施例提供的另一种网页安全处理装置对应的电子设备的结构

示意图，该电子设备可以包括：处理器41、存储器42，所述存储器42用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器41执行时实现前述各实施例中服务端所执行的各步骤。

[0081] 可选地，该电子设备中还可以包括通信接口43，用于与其他设备进行通信。

[0082] 另外，本发明实施例提供了一种计算机存储介质，用于储存计算机程序，该计算机程序使客户端执行时实现上述图3所示实施例中的网页安全处理方法。

[0083] 基于上述实施例，响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌；基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌；响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页。通过上述方案，在打开网页的时候，为了避免网页令牌等相关安全信息被泄露，及时清除网页本地缓存中的网页令牌等相关安全信息，在网页关闭的时候，在将网页令牌等安全相关信息存储回网页本地缓存中，以便下次可以顺利打开网页，即便在网页打开期间，也无法从网页本地缓存中获取到网页令牌等相关安全信息，能够有效确保网页使用安全，确保用户个人信息安全。既能确保用户在浏览网页的时候的信息安全防护效果，又能够不对用户的使用操作产生不利影响。

[0084] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0085] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助加必需的通用硬件平台的方式来实现，当然也可以通过硬件和软件结合的方式来实现。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以计算机产品的形式体现出来，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0086] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程资源更新设备的处理器以产生一个机器，使得通过计算机或其他可编程资源更新设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0087] 这些计算机程序指令也可存储在能引导计算机或其他可编程资源更新设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0088] 这些计算机程序指令也可装载到计算机或其他可编程资源更新设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一

个方框或多个方框中指定的功能的步骤。

[0089] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0090] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0091] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0092] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

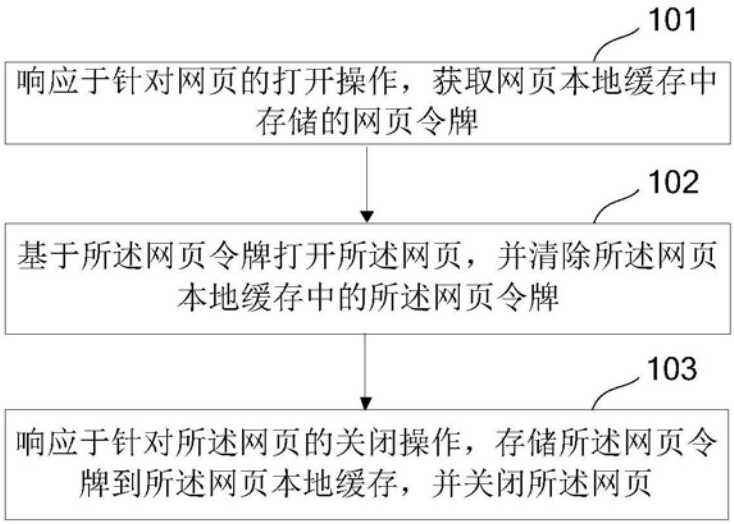

101
响应于针对网页的打开操作，获取网页本地缓存中存储的网页令牌
102
基于所述网页令牌打开所述网页，并清除所述网页本地缓存中的所述网页令牌
103
响应于针对所述网页的关闭操作，存储所述网页令牌到所述网页本地缓存，并关闭所述网页

图1

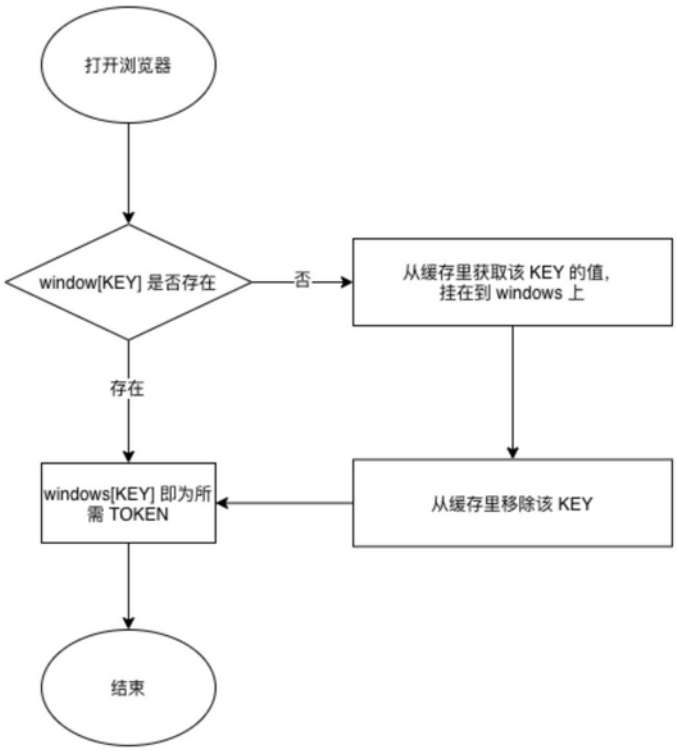

打开浏览器
window[KEY] 是否存在
否
从缓存里获取该 KEY 的值，挂在到 windows 上
存在
windows[KEY] 即为所需 TOKEN
从缓存里移除该 KEY
结束

图2a

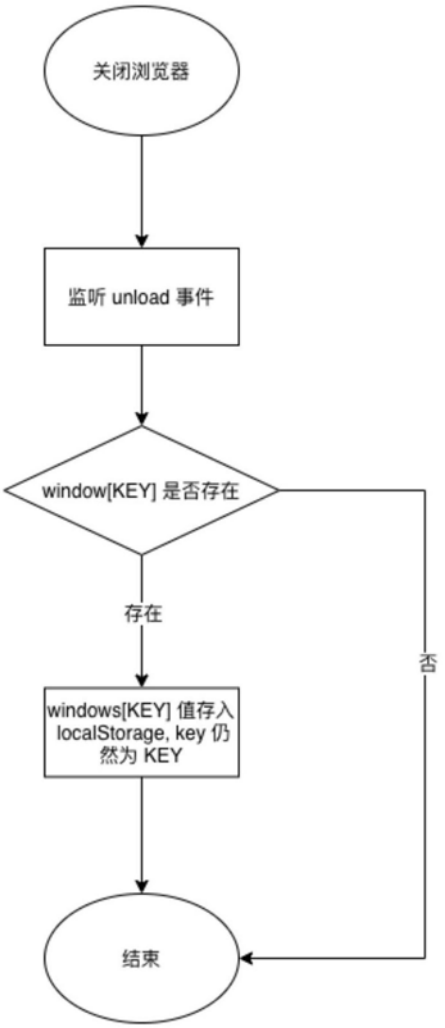

关闭浏览器
监听 unload 事件
window[KEY] 是否存在
存在
否
windows[KEY] 值存入 localStorage, key 仍然为 KEY
结束

图2b

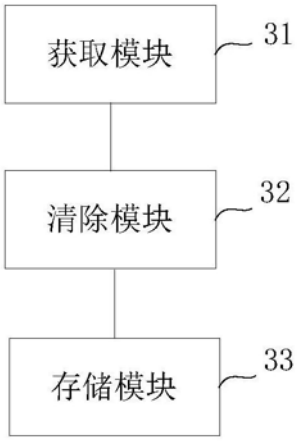

获取模块
31
清除模块
32
存储模块
33

图3

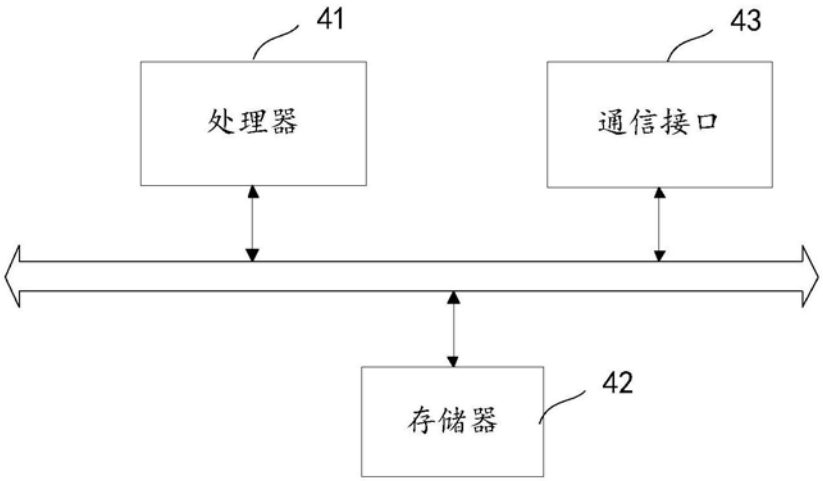


图4