(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115333828 A
(43)申请公布日 2022.11.11

(21)申请号 202210962563.3

(22)申请日 2022.08.11

(71)申请人 沈阳风驰软件股份有限公司
地址 110167 辽宁省沈阳市浑南区上深沟村861-17号(3门)

(72)发明人 裴志伟 贾正锋

(74)专利代理机构 辽宁惟则知识产权代理事务所(普通合伙) 21273
专利代理师 李巨智

(51)Int.Cl.
*H04L 9/40*(2022.01)
*H04L 9/32*(2006.01)
*H04L 67/02*(2022.01)
*H04L 69/16*(2022.01)

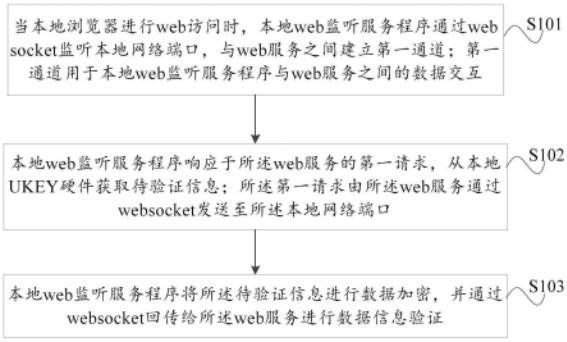
权利要求书2页 说明书8页 附图2页

(54)发明名称

基于UKEY硬件的web访问安全加密验证方法和设备

(57)摘要

本发明提供了基于UKEY硬件的web访问安全加密验证方法和设备。方法包括当本地浏览器进行web访问时,通过本地web监听服务程序建立本地UKEY硬件与web服务进行信息交互的通道,本地web监听服务程序通过websocket监听本地网络端口,web服务请求获取本地UKEY硬件相关信息,本地web监听服务程序以信息数据加密方式通过websocket回传web服务进行数据信息验证。以此方式,可以替代传统的web访问需要通过本地浏览器安装ActiveX插件方式与硬件交互,解决传统方式的安装ActiveX插件带来的安全问题、浏览器版本对ActiveX插件的兼容性问题以及浏览器对ActiveX插件逐渐不再支持从而影响正常使用的问题。




CN 115333828 A

1.一种基于UKEY硬件的web访问安全加密验证方法,其特征在于,包括:

当本地浏览器进行web访问时,本地web监听服务程序通过websocket监听本地网络端口,与web服务之间建立第一通道;所述第一通道用于本地web监听服务程序与web服务之间的数据交互;

所述本地web监听服务程序响应于所述web服务的第一请求,从本地UKEY硬件获取待验证信息;所述第一请求由所述web服务通过websocket发送至所述本地网络端口;

所述本地web监听服务程序将所述待验证信息进行数据加密,并通过websocket回传给所述web服务进行数据信息验证。

2.根据权利要求1所述的方法,其特征在于,所述本地web监听服务程序通过websocket监听本地网络端口,包括:

所述本地web监听服务程序创建网络端口列表;所述网络端口列表包括若干个网络端口地址,且相邻两个网络端口地址之间相差固定偏移值;

所述本地web监听服务程序与所述web服务对于所述网络端口列表协商一致;

所述本地web监听服务程序以所述网络端口列表的起始端口开始创建websocket服务端;websocket服务端用于监听所述本地网络端口;若当前网络端口被占用,则以当前网络端口增加固定偏移值后的网络端口重新创建websocket服务端,直至创建成功。

3.根据权利要求2所述的方法,其特征在于,本地web监听服务程序与web服务之间建立第一通道,包括:

本地浏览器通过向所述web服务请求数据,使web服务获取到本地socket网络通信数据,所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道。

4.根据权利要求3所述的方法,其特征在于,所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道,包括:

所述web服务创建websocket客户端,对所述网络端口列表进行扫描,从起始端口地址开始以固定偏移值尝试与所述本地web监听服务建立的websocket服务端建立网络连接,若当前网络端口建立网络连接失败,则以当前网络端口增加固定偏移值后的网络端口重新建立websocket的网络连接,直至成功创建所述web服务与所述本地web监听服务程序的网络连接,完成建立所述第一通道。

5.根据权利要求1所述的方法,其特征在于,还包括:

当本地浏览器访问web主页时,所述本地浏览器调用所述本地web监听服务程序提供的本地web服务接口,根据所述本地web服务接口的返回值判断所述本地web监听服务程序的状态,若检测到所述本地web监听服务程序处于运行状态,则不进行任何启动动作;若所述本地web监听服务程序处于未运行状态,通过调用URL协议启动运行所述本地web监听服务程序,使所述本地web监听服务程序重新建立websocket服务端,与所述web服务之间重新建立第一通道。

6.根据权利要求1所述的方法,其特征在于,还包括:

所述web服务向所述本地web监听服务程序周期性发送心跳数据包,以检测本地web监听服务程序的运行状态;

若未收到所述本地web监听服务程序回包数据的次数超过预设次数阈值,则判定所述

本地web监听服务程序处于未运行状态，所述web服务通过本地浏览器调用URL协议启动运行所述本地web监听服务程序，使所述本地web监听服务程序重新建立websocket服务端，与所述web服务之间重新建立第一通道。

7.根据权利要求1所述的方法，其特征在于，还包括：

所述本地web监听服务程序通过调用所述UKEY硬件的SDK接口获取所述UKEY硬件的状态，并将所述UKEY硬件的状态通过websocket返回所述web服务；若UKEY处于在线状态，则根据所述浏览器页面跳转请求执行浏览器页面跳转；若UKEY处于离线状态，则不执行浏览器页面跳转。

8.根据权利要求1所述的方法，其特征在于，所述数据信息验证，包括：

所述web服务将加密后的所述待验证信息进行解密，并将所述待验证信息与web服务数据库中的对应信息进行验证；所述待验证信息包括登录用户信息和用户访问权限ID信息；

若所述登录用户信息与web服务数据库中对应的登录用户信息一致，则执行浏览器页面访问；否则，不执行浏览器页面访问；

当执行浏览器页面访问时，根据所述用户访问权限ID信息获取web服务数据库中对应ID的用户访问权限，根据用户访问权限执行浏览器页面访问。

9.一种电子设备，包括至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其特征在于，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求1-8中任一项所述的方法。

# 基于UKEY硬件的web访问安全加密验证方法和设备

## 技术领域

[0001] 本发明一般涉及互联网技术领域,并且更具体地,涉及基于UKEY硬件的web访问安全加密验证方法和设备。

## 背景技术

[0002] 为了访问BS架构的web服务系统的安全性,一般需要对登录用户的身份进行验证,用户的身份信息验证通过后才能允许对系统的进一步操作,从而保证登录用户的合法性。目前传统的web服务用户登录验证基本有两种方式:一是通过在浏览器输入登录用户信息并通过软件加密进行后台验证方式;二是采用UKEY将用户信息存储于UKEY中,用户在通过指定浏览器进行登录时,通过ActiveX控件与UKEY进行信息验证。

[0003] 然而,以上两种验证方式均存在一定的安全隐患:

[0004] 第一种验证方式,虽然在与后台服务信息交互过程中将数据进行了软件加密处理,有效保护了用户的信息数据在传输过程中的安全性,但无法对使用该登录用户信息的使用者的身份合法性进行验证,可能会存在非法人员盗用其他合法人员的信息进行系统访问,从而影响整个系统的安全性。

[0005] 第二种验证方式,虽然采用了UKEY对用户信息使用者的合法性进行了限制,但此种方式需指定浏览器的版本,并要求浏览器允许通过ActiveX插件方式进行与UKEY硬件进行交互,除了浏览器版本的限制给用户的使用不友好的体验外,ActiveX插件本身就存在很严重的安全隐患,很容易被植入病毒软件盗取UKEY的用户信息,甚至对整个操作系统的安全性造成威胁,浏览器厂家也意识到了这种ActiveX插件的安全隐患问题,陆续对ActiveX的支持做了限制,甚至不再支持ActiveX插件,导致浏览器无法与UKEY进行数据交互,从而不能用此种方式进行用户信息的验证,最终无法对web系统进行访问。

## 发明内容

[0006] 根据本发明的实施例,提供了一种基于UKEY硬件的web访问安全加密验证方案。本方案有效解决了传统的访问web系统用户登录合法性验证的安全隐患和浏览器对ActiveX插件陆续不支持而导致无法正常访问web系统的风险,采用软件加密和硬件身份信息验证结合的方式,对使用用户登录信息的人员身份的安全性进行控制,可有效防止其他非法人员盗用合法身份信息登录系统,防止非法访问web服务对整个系统产生的安全隐患。

[0007] 在本发明的第一方面,提供了一种基于硬件的web访问安全加密验证方法。该方法包括:

[0008] 当本地浏览器进行web访问时,本地web监听服务程序通过websocket监听本地网络端口,与web服务之间建立第一通道;所述第一通道用于本地web监听服务程序与web服务之间的数据交互;

[0009] 所述本地web监听服务程序响应于所述web服务的第一请求,从本地UKEY硬件获取待验证信息;所述第一请求由所述web服务通过websocket发送至所述本地网络端口;

[0010] 所述本地web监听服务程序将所述待验证信息进行数据加密，并通过websocket回传给所述web服务进行数据信息验证。

[0011] 进一步地，所述本地web监听服务程序通过websocket监听本地网络端口，包括：

[0012] 所述本地web监听服务程序创建网络端口列表；所述网络端口列表包括若干个网络端口地址，且相邻两个网络端口地址之间相差固定偏移值；

[0013] 所述本地web监听服务程序与所述web服务对于所述网络端口列表协商一致；

[0014] 所述本地web监听服务程序以所述网络端口列表的起始端口开始创建websocket服务端；websocket服务端用于监听所述本地网络端口；若当前网络端口被占用，则以基于当前网络端口增加固定偏移值后的网络端口重新创建websocket服务端，直至创建成功。

[0015] 进一步地，本地web监听服务程序与web服务之间建立第一通道，包括：

[0016] 本地浏览器通过向所述web服务请求数据，使web服务获取到本地socket网络通信数据，所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道。

[0017] 进一步地，所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道，包括：

[0018] 所述web服务创建websocket客户端，对所述网络端口列表进行扫描，从起始端口地址开始以固定偏移值尝试与所述本地web监听服务建立的websocket服务端建立网络连接，若当前网络端口建立网络连接失败，则以当前网络端口增加固定偏移值后的网络端口重新建立websocket的网络连接，直至建立成功创建所述web服务与所述本地web监听服务程序的网络连接，完成建立所述第一通道。

[0019] 进一步地，还包括：

[0020] 当本地浏览器访问web主页时，所述本地浏览器调用所述本地web监听服务程序提供的本地web服务接口，根据所述本地web服务接口的返回值判断所述本地web监听服务程序的状态，若检测到所述本地web监听服务程序处于运行状态，则不进行任何启动动作；若所述本地web监听服务程序处于未运行状态，通过调用URL协议启动运行所述本地web监听服务程序，使所述本地web监听服务程序重新建立websocket服务端，与所述web服务之间重新建立第一通道。

[0021] 进一步地，还包括：

[0022] 所述web服务向所述本地web监听服务程序周期性发送心跳数据包，以检测本地web监听服务程序的运行状态；

[0023] 若未收到所述本地web监听服务程序回包数据的次数超过预设次数阈值，则判定所述本地web监听服务程序处于未运行状态，所述web服务通过本地浏览器调用URL协议启动运行所述本地web监听服务程序，使所述本地web监听服务程序重新建立websocket服务端，与所述web服务之间重新建立第一通道。

[0024] 进一步地，还包括：

[0025] 所述本地web监听服务程序通过调用所述UKEY硬件的SDK接口获取所述UKEY硬件的状态，并将所述UKEY硬件的状态通过websocket返回所述web服务；若UKEY处于在线状态，则根据所述浏览器页面跳转请求执行浏览器页面跳转；若UKEY处于离线状态，则不执行浏览器页面跳转。

[0026] 进一步地,所述数据信息验证,包括:

[0027] 所述web服务将加密后的所述待验证信息进行解密,并将所述待验证信息与web服务数据库中的对应信息进行验证;所述待验证信息包括登录用户信息和用户访问权限ID信息;

[0028] 若所述登录用户信息与web服务数据库中对应的登录用户信息一致,则执行浏览器页面访问;否则,不执行浏览器页面访问;

[0029] 当执行浏览器页面访问时,根据所述用户访问权限ID信息获取web服务数据库中对应ID的用户访问权限,根据用户访问权限执行浏览器页面访问。

[0030] 在本发明的第二方面,提供了一种电子设备。该电子设备至少一个处理器;以及与所述至少一个处理器通信连接的存储器;所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行本发明第一方面的方法。

[0031] 应当理解,发明内容部分中所描述的内容并非旨在限定本发明的实施例的关键或重要特征,亦非用于限制本发明的范围。本发明的其它特征将通过以下的描述变得容易理解。

## 附图说明

[0032] 结合附图并参考以下详细说明,本发明各实施例的上述和其他特征、优点及方面将变得更加明显。在附图中,相同或相似的附图标记表示相同或相似的元素,其中:

[0033] 图1示出了根据本发明的实施例的基于UKEY硬件的web访问安全加密验证方法的流程图;

[0034] 图2示出了根据本发明的实施例的本地web监听服务程序监听本地网络端口的流程图;

[0035] 图3示出了能够实施本发明的实施例的示例性电子设备的方框图;

[0036] 其中,300为电子设备、301为CPU、302为ROM、303为RAM、304为总线、305为I/O接口、306为输入单元、307为输出单元、308为存储单元、309为通信单元。

## 具体实施方式

[0037] 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作出创造性劳动前提下所获得的全部其他实施例,都属于本发明保护的范围。

[0038] 另外,本文中术语“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。

[0039] 本发明中,采用在一个本地web监听服务程序侧创建websocket服务端,与web服务侧创建的websocket客户端建议通信通道,使UKEY硬件与本地浏览器应用的信息交互建立通信桥梁,接收处理web服务系统的验证请求信息,从UKEY硬件中获取请求数据,并回传给web服务进行信息验证。

[0040] 图1示出了本发明实施例的基于UKEY硬件的web访问安全加密验证方法的流程图。

[0041] 该方法包括：

[0042] S101、当本地浏览器进行web访问时，本地web监听服务程序通过websocket监听本地网络端口，与web服务之间建立第一通道；所述第一通道用于本地web监听服务程序与web服务之间的数据交互。

[0043] 进一步地，所述本地web服务程序与所述web服务协商以JSON数据结构进行数据交互。

[0044] 作为本发明的一种实施例，如图2所示，本地web监听服务程序通过websocket监听本地网络端口，包括：

[0045] S201、所述本地web监听服务程序创建网络端口列表。

[0046] 所述网络端口列表包括若干个网络端口地址，且相邻两个网络端口地址之间相差固定偏移值。

[0047] TCP/IP协议中规定网络端口取值范围为0～65535，其中，1024到5000作为临时端口可供用户应用程序使用。在本实施例中，从1024到5000临时端口范围内，以2021作为起始端口，以依次增加51的固定偏移值的端口作为下一个端口，一共取出20个端口组成所述网络端口列表。

[0048] 设置网络端口列表，能够保证本地web监听服务程序websocket成功监听本地网络端口，防止某个监听端口被占用。

[0049] S202、所述本地web监听服务程序与所述web服务对于所述网络端口列表协商一致。

[0050] 在本实施例中，所述本地web监听服务程序与所述web服务事先协商基于同一范围内的网络端口，并以同一固定偏移值增加网络端口进行创建websocket的网络连接。

[0051] S203、所述本地web监听服务程序以所述网络端口列表的起始端口开始创建websocket服务端；websocket服务端用于监听所述本地网络端口；若当前网络端口被占用，则增加固定偏移值重新创建websocket本地网络端口的监听，直至创建成功。

[0052] 在本实施例中，所述固定偏移值可以选定为51，若当前网络端口被占用，则通过增加51偏移值，对网络端口列表中的下一网络端口创建websocket服务端，直至创建成功。

[0053] 作为本发明的一种实施例，所述本地web监听服务程序与web服务之间建立第一通道，包括：

[0054] 本地浏览器通过向所述web服务请求数据，使web服务获取到本地socket网络通信数据，所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道。

[0055] 在本实施例中，所述web服务根据获取到的本地socket网络通信数据建立与所述本地web监听服务程序的第一通道，包括：

[0056] 所述web服务创建websocket客户端，对所述网络端口列表进行扫描，从起始端口地址开始以固定偏移值尝试与所述本地web监听服务建立的websocket服务端建立网络连接。若当前网络端口建立网络连接失败，则增加固定偏移值与其他网络端口建立websocket的网络连接，直至成功创建与所述本地web监听服务程序的网络连接，完成建立所述第一通道。

[0057] 在本地浏览器进行web访问时，如果本地web监听服务程序处于未启动运行状态，则无法与web服务之间进行数据交互，故当本地浏览器访问web主页时，所述本地浏览器根据调用所述本地web监听服务程序提供的本地web服务接口的返回值判断所述本地web监听服务程序是否处于运行状态。在本实施例中，如果返回值为200，则调用成功，即本地web监听服务程序处于运行状态。如果返回值不为200，则调用失败，即本地web监听服务程序处于未运行状态。

[0058] 进一步地，若检测到所述本地web监听服务程序处于运行状态，则不进行任何启动动作；若所述本地web监听服务程序处于未运行状态，通过调用URL协议启动运行所述本地web监听服务程序。

[0059] 在上述实施例中，URL协议为自定义的URL协议；具体是本地web监听服务程序的安装脚本在初次安装在运行系统时，向注册表中注册的一个自定义URL协议。通过将自定义URL协议注册到本地系统注册表中，所述自定义URL协议在注册表中与本地应用程序exe文件安装路径相关联，使得本地浏览器可通过注册后的URL启动本地应用程序。注册的URL格式定义为:自定义协议名称://参数1名称＝参数1值&参数2名称＝参数2值.....。所述本地浏览器通过调用<a href＝"customAPP://param1＝1&param2＝2"/>举例格式脚本启动运行本地web监听服务程序。

[0060] 通过在本地浏览器访问web主页时检测本地web监听服务程序的状态，能够有效保证在首次登录web主页进行访问时，本地web监听服务程序与web服务之间建立有效可用的数据信息交互通道，保证访问web主页时进行登录用户信息的交互验证和后续访问web的数据交互验证。

[0061] 作为本发明的一种实施例，在所述本地web监听服务程序创建的websocket服务端与所述web服务创建的websocket客户端建立网络连接后，所述web服务通过websocket向所述本地web监听服务程序周期性发送心跳数据包，以检测本地web监听服务程序的运行状态；通过预设次数阈值，若未收到所述本地web监听服务程序回包数据的次数超过预设次数阈值，则判定所述本地web监听服务程序处于未运行状态，所述web服务通过本地浏览器调用URL协议启动运行所述本地web监听服务程序，使所述本地web监听服务程序通过websocket监听本地网络端口，与web服务之间重新建立第一通道。

[0062] 在上述实施例中，URL协议为自定义的URL协议；具体是本地web监听服务程序的安装脚本在初次安装在运行系统时，向注册表中注册的一个自定义的URL协议。通过将自定义URL协议注册到本地系统注册表中，所述自定义URL协议在注册表中与本地应用程序exe文件安装路径相关联，使得本地浏览器可通过注册后的URL启动本地应用程序。注册的URL格式定义为:自定义协议名称://参数1名称＝参数1值&参数2名称＝参数2值.....。所述本地浏览器通过调用<a href＝"customAPP://param1＝1&param2＝2"/>举例格式脚本启动运行本地应用程序。

[0063] 通过web服务发送心跳数据包，以检测本地web监听服务程序的运行状态，能够在检测到本地web监听服务程序处于未运行状态时，提供一种重新启动本地web监听服务程序的机制方法，保证在访问web过程中所述本地web监听服务程序始终处于运行状态，从而保证所述web服务与所述本地web监听服务程序建立有效可用的网络通道进行数据交互，使所述web服务终于可以对访问web进行数据信息验证，保证访问web的安全性。

[0064] S102、所述本地web监听服务程序响应于所述web服务的第一请求，从本地UKEY硬件获取待验证信息；所述第一请求由所述web服务通过websocket发送至所述本地网络端口。

[0065] 所述第一请求包括请求获取的待验证信息类别。所述待验证信息包括登录用户信息和用户访问权限ID信息。所述登录用户信息，例如用户ID、登录用户名、登录密码。

[0066] 在本实施例中，响应于第一请求，能够从本地UKEY硬件中获取登录用户信息和/或用户访问权限ID信息。

[0067] 在一些实施例中，可能会存在UKEY硬件离线的情况，导致无法获取待验证信息。在上述实施例中，本地web监听服务程序通过所述UKEY硬件的SDK接口获取所述UKEY硬件的状态，并将所述UKEY硬件的状态通过websocket返回web服务；若UKEY处于在线状态，则根据所述浏览器页面访问请求执行浏览器页面访问；若UKEY处于离线状态，则不执行浏览器页面访问。

[0068] 通过上述实施例中对UKEY硬件在线或离线状态的验证，能够有效防止在UKEY合法使用者已成功通过登录信息验证后，访问web页面未关闭情况下并且UKEY硬件处于离线状态时，非UKEY合法使用者利用合法用户身份继续对页面的访问，从而可能给web系统造成安全性问题。

[0069] S103、所述本地web监听服务程序将所述待验证信息进行数据加密，并通过websocket回传给所述web服务进行数据信息验证。

[0070] 作为本发明的一种实施例，可以通过将JSON数据结构通过字符串混淆算法进行数据加密传输，接收方以同样的字符串混淆算法进行解密，实现数据传输的加解密过程。

[0071] 作为本发明的一种实施例，所述数据信息验证，包括：

[0072] 所述web服务将所述待验证信息与web服务数据库中的对应信息进行验证；所述待验证信息包括登录用户信息和用户访问权限ID信息。若所述登录用户信息与web服务数据库中对应的登录用户信息一致，则执行浏览器页面访问；否则，不执行浏览器页面访问。

[0073] 具体地，若登录用户信息验证一致，则允许所述浏览器页面访问请求，执行浏览器页面访问；若信息验证不一致则不执行浏览器页面访问，提示用户信息验证失败。

[0074] 进一步地，当执行浏览器页面访问时，根据所述用户访问权限ID信息获取web服务数据库中对应ID的用户访问权限，根据用户访问权限执行浏览器页面访问。

[0075] 具体地，在所述浏览器执行页面访问时，根据获取到的UEKY中存储的用户访问权限ID信息数据，从数据库中获取对应的访问权限，来控制所述登录用户所能访问页面的权限。所述访问权限包括是否允许对web的访问，以及对每个页面内的模块是否展示给用户和是否具有对某个页面功能进行操作的权限。

[0076] 通过上述实施例的方式，对使用用户登录信息的人员身份的安全性进行有限控制，可有效防止其他非法人员盗用合法身份信息登录系统，防止非法访问web服务对整个系统产生的安全隐患，有效解决了传统的访问web系统用户登录合法性验证的安全隐患问题，同时还避免了浏览器对ActiveX插件陆续不支持而导致无法正常访问web系统的风险。

[0077] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，所述描述的模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0078] 本发明的技术方案中，所涉及的用户个人信息的获取，存储和应用等，均符合相关

法律法规的规定，且不违背公序良俗。

[0079] 根据本发明的实施例，本发明还提供了一种电子设备和一种可读存储介质。

[0080] 图3示出了可以用来实施本发明的实施例的电子设备300的示意性框图。电子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或者要求的本发明的实现。

[0081] 设备300包括计算单元301，其可以根据存储在只读存储器(ROM)302中的计算机程序或者从存储单元308加载到随机访问存储器(RAM)303中的计算机程序，来执行各种适当的动作和处理。在RAM 303中，还可存储设备300操作所需的各种程序和数据。计算单元301、ROM 302以及RAM 303通过总线304彼此相连。输入/输出(I/O)接口305也连接至总线304。

[0082] 设备300中的多个部件连接至I/O接口305，包括：输入单元306，例如键盘、鼠标等；输出单元307，例如各种类型的显示器、扬声器等；存储单元308，例如磁盘、光盘等；以及通信单元309，例如网卡、调制解调器、无线通信收发机等。通信单元309允许设备300通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0083] 计算单元301可以是各种具有处理和计算能力的通用和/或专用处理组件。计算单元301的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的计算单元、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。计算单元301执行上文所描述的各个方法和处理，例如方法S101～S103。例如，在一些实施例中，方法S101～S103可被实现为计算机软件程序，其被有形地包含于机器可读介质，例如存储单元308。在一些实施例中，计算机程序的部分或者全部可以经由ROM 302和/或通信单元309而被载入和/或安装到设备300上。当计算机程序加载到RAM 303并由计算单元301执行时，可以执行上文描述的方法S101～S103的一个或多个步骤。备选地，在其他实施例中，计算单元301可以通过其他任何适当的方式(例如，借助于固件)而被配置为执行方法S101～S103。

[0084] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、负载可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0085] 用于实施本发明的方法的程序代码可以采用一个或多个编程语言的任何组合来编写。这些程序代码可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器或控制器，使得程序代码当由处理器或控制器执行时使流程图和/或框图中所规定的功能/操作被实施。程序代码可以完全在机器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0086] 在本发明的上下文中，机器可读介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0087] 为了提供与用户的交互，可以在计算机上实施此处描述的系统和技术，该计算机具有：用于向用户显示信息的显示装置(例如，CRT(阴极射线管)或者LCD(液晶显示器)监视器)；以及键盘和指向装置(例如，鼠标或者轨迹球)，用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈(例如，视觉反馈、听觉反馈、或者触觉反馈)；并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0088] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如，作为数据服务器)、或者包括中间件部件的计算系统(例如，应用服务器)、或者包括前端部件的计算系统(例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如，通信网络)来将系统的部件相互连接。通信网络的示例包括：局域网(LAN)、广域网(WAN)和互联网。

[0089] 计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，也可以为分布式系统的服务器，或者是结合了区块链的服务器。

[0090] 应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本发明中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本发明的技术方案所期望的结果，本文在此不进行限制。

[0091] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，根据设计要求和其他因素，可以进行各种修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

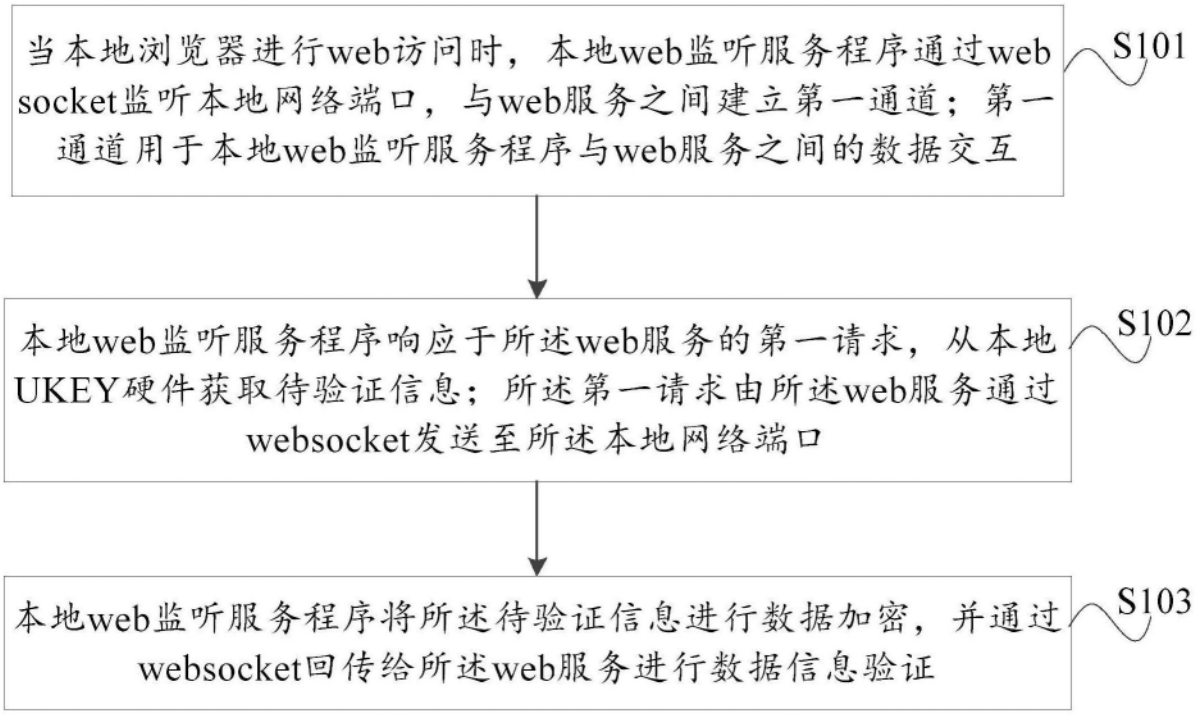

当本地浏览器进行web访问时，本地web监听服务程序通过web socket监听本地网络端口，与web服务之间建立第一通道；第一通道用于本地web监听服务程序与web服务之间的数据交互
S101
本地web监听服务程序响应于所述web服务的第一请求，从本地UKEY硬件获取待验证信息；所述第一请求由所述web服务通过websocket发送至所述本地网络端口
S102
本地web监听服务程序将所述待验证信息进行数据加密，并通过websocket回传给所述web服务进行数据信息验证
S103

图1

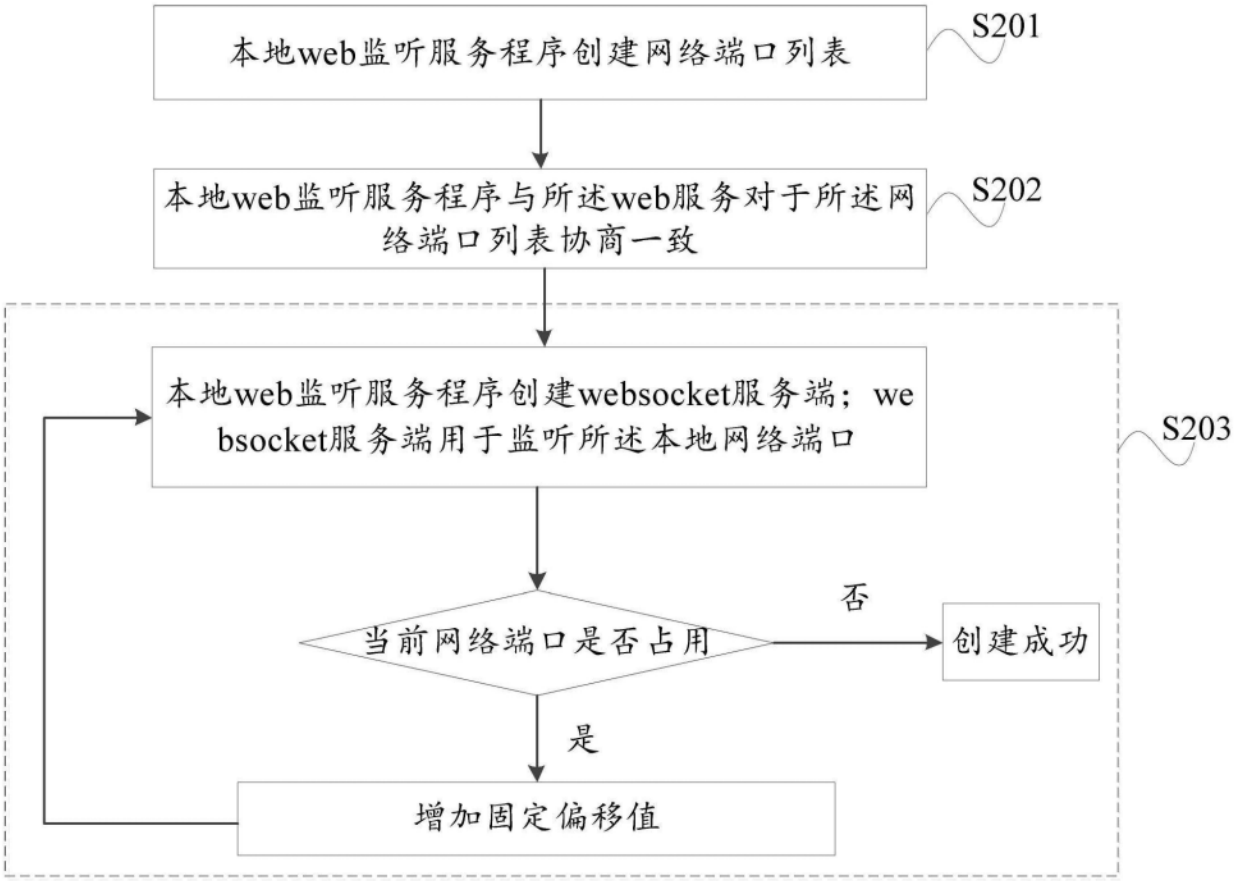

本地web监听服务程序创建网络端口列表
S201
本地web监听服务程序与所述web服务对于所述网络端口列表协商一致
S202
本地web监听服务程序创建websocket服务端；websocket服务端用于监听所述本地网络端口
S203
当前网络端口是否占用
否
创建成功
是
增加固定偏移值

图2

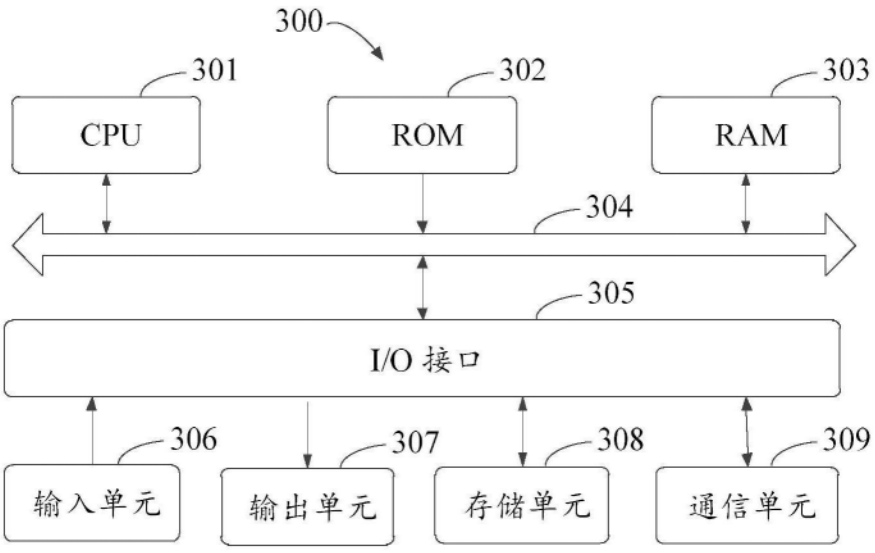

300
301
CPU
302
ROM
303
RAM
304
305
I/O 接口
306
输入单元
307
输出单元
308
存储单元
309
通信单元

图3