[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公布说明书

[21] 申请号 200810142092.1

[43] 公开日 2010 年 3 月 3 日

[11] 公开号 CN 101662457A

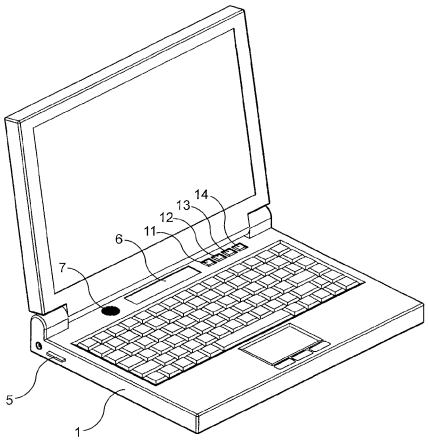
[22] 申请日 2008.8.28
[21] 申请号 200810142092.1
[71] 申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层
[72] 发明人 黄金富
权利要求书 4 页 说明书 7 页 附图 1 页

[54] 发明名称

一种设有网络数据过滤装置的笔记本型计算机

[57] 摘要

一种设有网络数据过滤装置的笔记本型计算机，除了具备一般笔记本型计算机的软硬件外，还设有独立网络数据过滤装置，所述网络数据过滤装置包括控制器(2)、计算机端网络接口(3)、网络端网络接口(4)、储存装置(5)、显示装置(6)、发声装置(7)、可信任按键(11)、不信任按键(12)、临时信任按键(13)、总开关(14)，其中，储存装置(5)内储存有可信任 IP 地址和不信任 IP 地址，控制器(2)按预定程序运作，将计算机与外部网络之间传送的数据包进行过滤，拦截所有与不信任 IP 地址通讯的数据包，使笔记本型计算机连线上网时，只能与信任的 IP 地址进行交换信息，保障机内资料不会被人盗取传送到非信任的 IP 地址。



1. 一种设有网络数据过滤装置的笔记本型计算机，所述的计算机除了具备一般笔记本型计算机所具备的软硬件外，还设有独立的网络数据过滤装置，其特征在于，所述的网络数据过滤装置包括有控制器（2）、计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14），其中，控制器（2）分别与计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14）等相电路连接，储存装置（5）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（2）按预定程序运作，将从计算机端网络接口（3）传送给网络端网络接口（4）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（4）传送给计算机端网络接口（3）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

2. 如权利要求 1 所述的笔记本型计算机，其特征在于，所述的储存装置（5）内还储存有多个 IP 地址对应的网域名称资料，包括各个可信任 IP 地址对应的网域名称资料、各个不信任 IP 地址对应的网域名称资料、其他 IP 地址对应的网域名称资料。

3. 如权利要求 1 所述的笔记本型计算机，其特征在于，所述的总开关（14）是所述的网络数据过滤装置的总开关。

4. 如权利要求 1 或 2 或 3 所述的笔记本型计算机，其特征在于，当所述的控制器（2）从计算机端网络接口（3）接收到数据包时，控制器（2）将该数据包的目的地 IP 地址与储存装置（5）所储存的各个可信任 IP

地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 A 组程序的其中一个程序：

程序 A1：当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同时，控制器（2）将该数据包拦截弃掉，并通过发声装置（7）发出告警提示声音 和/或 通过显示装置（6）显示该不信任 IP 地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称；

程序 A2：当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同时，控制器（2）将该数据包输出到网络端网络接口（4）；

程序 A3：当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，控制器（2）通过发声装置（7）发出提示声音 和/或 通过显示装置（6）显示该陌生 IP 地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称。

5. 如权利要求 4 所述的网络数据过滤装置，其特征在于，当控制器（2）执行所述的程序 A3 后，控制器（2）等待接收用户的按键操作，当用户按下可信任按键（11）、不信任按键（12）、临时信任按键（13）等的其中一个按键，控制器（2）执行包括如下的 B 组程序的其中一个程序：

程序 B1：当用户按下不信任按键（12），控制器（2）将该数据包拦截弃掉，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到储存装置（5）中；

程序 B2：当用户按下可信任按键（11），控制器（2）将该数据包输出到网络端网络接口（4），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中；

程序 B3：当用户按下临时信任按键（13），控制器（2）将该数据包输出到网络端网络接口（4），然后控制器（2）将所述的陌生 IP 地址设定为可信任 IP 地址储存到储存装置（5）中，并设定该可信任 IP 地址的有效时间，以及，控制器（2）在该有效时间过后从储存装置（5）中删除该可信任 IP 地址。

6. 如权利要求 1 或 2 或 3 所述的笔记本型计算机，其特征在于，当所述的控制器（2）从网络端网络接口（4）接收到数据包时，控制器（2）将该数据包的来源地 IP 地址与储存装置（5）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 C 组程序的其中一个程序：

程序 C1：当数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，控制器（2）将该数据包拦截弃掉，并通过发声装置（7）发出告警提示声音 和/或 通过显示装置（6）显示该不信任 IP 地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称；

程序 C2：当数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，控制器（2）将该数据包输出到计算机端网络接口（3）；

程序 C3：当数据包的来源地 IP 地址与任何一个可信任 IP 地址不相同，并且该来源地 IP 地址与任何一个不信任 IP 地址也不相同时，该来源地 IP 地址为陌生 IP 地址，控制器（2）通过发声装置（7）发出提示声音 和/或 通过显示装置（6）显示该陌生 IP

地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称。

7. 如权利要求 6 所述的网络数据过滤装置，其特征在于，当控制器（2）执行所述的程序 C3 后，控制器（2）等待接收用户的按键操作，当用户按下可信任按键（11）、不信任按键（12）、临时信任按键（13）等的其中一个按键，控制器（2）执行包括如下的 D 组程序的其中一个程序:

程序 D1: 当用户按下不信任按键（12），控制器（2）将该数据包拦截弃掉，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到储存装置（5）中;

程序 D2: 当用户按下可信任按键（11），控制器（2）将该数据包输出到计算机端网络接口（3），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中;

程序 D3: 当用户按下临时信任按键（13），控制器（2）将该数据包输出到计算机端网络接口（3），然后控制器（2）将所述的陌生 IP 地址设定为可信任 IP 地址储存到储存装置（5）中，并设定该可信任 IP 地址的有效时间，以及，控制器（2）在该有效时间过后从储存装置（5）中删除该可信任 IP 地址。

一种设有网络数据过滤装置的笔记本型计算机

【技术领域】

本发明涉及计算机和数据安全技术领域，特别是涉及一种设有网络数据过滤装置的笔记本型计算机。

【背景技术】

随着时代的进步，资讯科技的应用非常普及，尤其是计算机和互联网的发展，金融机构如银行等，提供了很多利用资讯科技的服务，例如网上银行服务、网上证券买卖服务等，这些服务一般是将用户的交易信息通过互联网传送到金融机构，由金融机构核实用户的交易信息后，根据交易信息内容进行相应的操作。由于这些交易信息内包含有用户的重要资料，例如账户号码、账户口令等，只要盗取得这些资料就可以在用户不知情下操控用户的账户，盗取用户账户内的钱，所以有些黑客通过各种各样的入侵方法，将木马程式置于用户的计算机内，在用户连线到金融机构的服务器时，通过木马程式盗取用户的资料，包括账户号码、账户口令等，然后将这些资料传送到黑客指定的服务器。由于木马程式平常是隐藏于计算机内，即使被黑客利用木马程式盗取了用户的资料，用户一般是不会察觉，黑客继而使用这些资料盗取用户的账户内的钱，令用户蒙受损失，是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种设有网络数据过滤装置的笔记本型计算机，使计算机连线上网与其他计算机通讯时，只能与用户信任的 IP 地址的计算机进行交换信息，从而使黑客不能通过木马程式将所盗取的资料传送到非用户信任的 IP 地址。

本发明的目的是这样实现的，采用这样一种设有网络数据过滤装置的笔记本型计算机，所述的计算机除了具备一般笔记本型计算机所具备的软硬件外，还设有独立的网络数据过滤装置，其特征在于，所述的网络数据过滤装置包括有控制器（2）、计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14），其中，控制器（2）分别与计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14）等相电路连接，储存装置（5）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（2）按预定程序运作，将从计算机端网络接口（3）传送给网络端网络接口（4）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（4）传送给计算机端网络接口（3）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

这样就实现了本发明的目的。

采用了本发明的笔记本型计算机，即使中了黑客的木马程式，当木马程式将所盗取的资料传送到黑客指定的 IP 地址时，网络数据过滤装置会即时发现该 IP 地址并非是用户所信任的 IP 地址，就不会让该资料传送到黑客指定的 IP 地址。

【附图说明】

图 1 是本发明的设有网络数据过滤装置的笔记本型计算机的形像化立体示意说明图；

图 2 是本发明的设有网络数据过滤装置的笔记本型计算机的结构示意说明图。

图中，相同的数字代表相同的系统、装置、部件器件，附图是示意性的，用以说明本发明的构成和主要特征。

【具体实施方式】

下面结合附图，对本发明的方法作进一步详细说明。

参阅图 1 和图 2，图 1 是本发明的设有网络数据过滤装置的笔记本型计算机的形像化立体示意说明图，图 2 是本发明的设有网络数据过滤装置的笔记本型计算机的结构示意说明图，图 1 和图 2 中示出的计算机除了具备一般笔记本型计算机所具备的软硬件外，还设有独立的网络数据过滤装置，所述的网络数据过滤装置包括有控制器（2）、计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14），其中，控制器（2）分别与计算机端网络接口（3）、网络端网络接口（4）、储存装置（5）、显示装置（6）、发声装置（7）、可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14）等相电路连接，储存装置（5）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（2）按预定程序运作，将从计算机端网络接口（3）传送给网络端网络接口（4）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（4）传送给计算机端网络接口（3）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

继续参阅图 1 和图 2，图 1 和图 2 中示出的笔记本型计算机的外壳（1）上设有四个网络数据过滤装置专用的按键，包括：可信任按键（11）、不信任按键（12）、临时信任按键（13）、总开关（14），其中总开关（14）是所述的网络数据过滤装置的总开关，其余的可信任按键（11）、不信任按键（12）、临时信任按键（13）等按键是用于指示控制器（2）如何处理陌生 IP 地址。

在本发明中，计算机端网络接口（3）是连接到计算机内部的网络接口电路，而网络端网络接口（4）是连接到计算机的网络插座，也就是网络数据过滤装置是置于计算机内部的网络接口与外部网络之间，由网络数据过滤装置对流过的数据进行过滤，包括从计算机端网络接口（3）传送给网络端网络接口（4）的数据包，和从网络端网络接口（4）传送给计算机端网络接口（3）的数据包，以下将分别作进一步详细说明。此外，储存装置（5）内还储存有多个 IP 地址对应的网域名称资料，包括各个可信任 IP 地址对应的网域名称资料、各个不信任 IP 地址对应的网域名称资料、其他 IP 地址对应的网域名称资料。

以下是使用本发明的笔记本型计算机上网时，网络数据过滤装置将计算机传送给网络的数据包进行过滤的过程，当所述的控制器（2）从计算机端网络接口（3）接收到数据包时，控制器（2）将该数据包的目的地 IP 地址与储存装置（5）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 A 组程序的其中一个程序：

程序 A1：当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同时，控制器（2）将该数据包拦截弃掉，并通过发声装置（7）发出告警提示声音 和/或 通过显示装置（6）显示该不信任 IP 地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称；

程序 A2：当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同时，控制器（2）将该数据包输出到网络端网络接口（4）；

程序 A3：当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，控制器（2）通过发声装置（7）发出提示声音 和/或 通过显示装置（6）显示该陌生 IP

地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称。

当控制器（2）执行所述的程序 A3 后，控制器（2）等待接收用户的按键操作，当用户按下可信任按键（11）、不信任按键（12）、临时信任按键（13）等的其中一个按键，控制器（2）执行包括如下的 B 组程序的其中一个程序：

程序 B1：当用户按下不信任按键（12），控制器（2）将该数据包拦截弃掉，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到储存装置（5）中；

程序 B2：当用户按下可信任按键（11），控制器（2）将该数据包输出到网络端网络接口（4），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中；

程序 B3：当用户按下临时信任按键（13），控制器（2）将该数据包输出到网络端网络接口（4），然后控制器（2）将所述的陌生 IP 地址即所述的数据包的目的地 IP 地址设定为可信任 IP 地址储存到储存装置（5）中，并设定该可信任 IP 地址的有效时间，以及，控制器（2）在该有效时间过后从储存装置（5）中删除该可信任 IP 地址。

以下是使用本发明的笔记本型计算机上网时，网络数据过滤装置将从外部网络传送给计算机的数据包进行过滤的过程，当所述的控制器（2）从网络端网络接口（4）接收到数据包时，控制器（2）将该数据包的来源地 IP 地址与储存装置（5）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 C 组程序的其中一个程序：

程序 C1：当数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，控制器（2）将该数据包拦截弃掉，并通过发声装置（7）发出告警提示声音 和/或 通过显示装置（6）显示该不信任 IP

地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称;

程序 C2: 当数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，控制器（2）将该数据包输出到计算机端网络接口（3）;

程序 C3: 当数据包的来源地 IP 地址与任何一个可信任 IP 地址不相同，并且该来源地 IP 地址与任何一个不信任 IP 地址也不相同时，该来源地 IP 地址为陌生 IP 地址，控制器（2）通过发声装置（7）发出提示声音 和/或 通过显示装置（6）显示该陌生 IP 地址的文字信息，所述的文字信息包括 IP 地址 和/或 该 IP 地址对应的网域名称。

当用户按下可信任按键（11）、不信任按键（12）、临时信任按键（13）等的其中一个按键，控制器（2）执行包括如下的 D 组程序的其中一个程序:

程序 D1: 当用户按下不信任按键（12），控制器（2）将该数据包拦截弃掉，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到储存装置（5）中;

程序 D2: 当用户按下可信任按键（11），控制器（2）将该数据包输出到计算机端网络接口（3），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中;

程序 D3: 当用户按下临时信任按键（13），控制器（2）将该数据包输出到计算机端网络接口（3），然后控制器（2）将所述的陌生 IP 地址即所述的数据包的目的地 IP 地址设定为可信任 IP 地址储存到储存装置（5）中，并设定该可信任 IP 地址的有效时间，以及，控制器（2）在该有效时间过后从储存装置（5）中删除该可信任 IP 地址。

继续参阅图 1，图 1 中示出的笔记本型计算机的网络数据过滤装置是采用记忆卡作为储存装置（5），可以预先将各个可信任 IP 地址及其对应的

网域名称、各个不信任 IP 地址及其对应的网域名称、其他 IP 地址及其对应的网域名称等等的资料写到记忆卡，然后才将记忆卡插到网络数据过滤装置上使用。

以上已经详细说明了本发明的设有网络数据过滤装置的笔记本型计算机，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

本发明的设有网络数据过滤装置的笔记本型计算机是采用一个独立于计算机主板的网络数据过滤装置，与计算机主板是物理上隔离的，即使笔记本型计算机感染了病毒和木马程式，也不会影响网络数据过滤装置的工作。本发明的实施，保障了用户的资料不会被木马程式盗走，特别适合应用于一些经常连线到金融网站的应用。

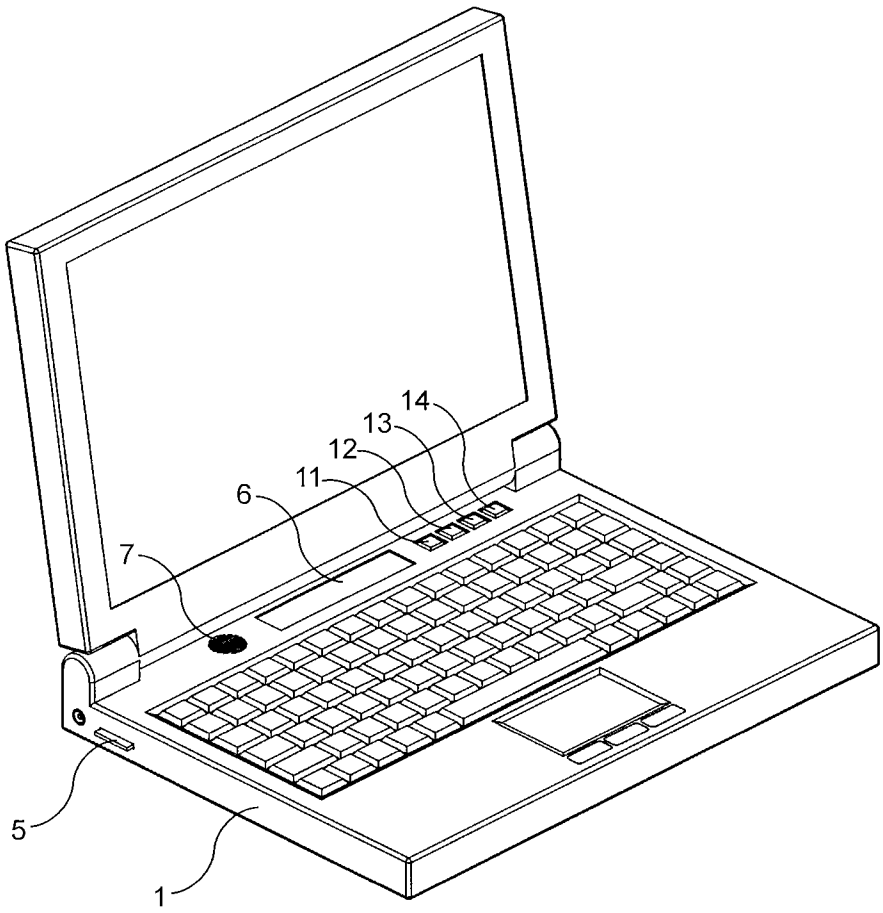

14
13
12
11
6
7
5
1

图 1

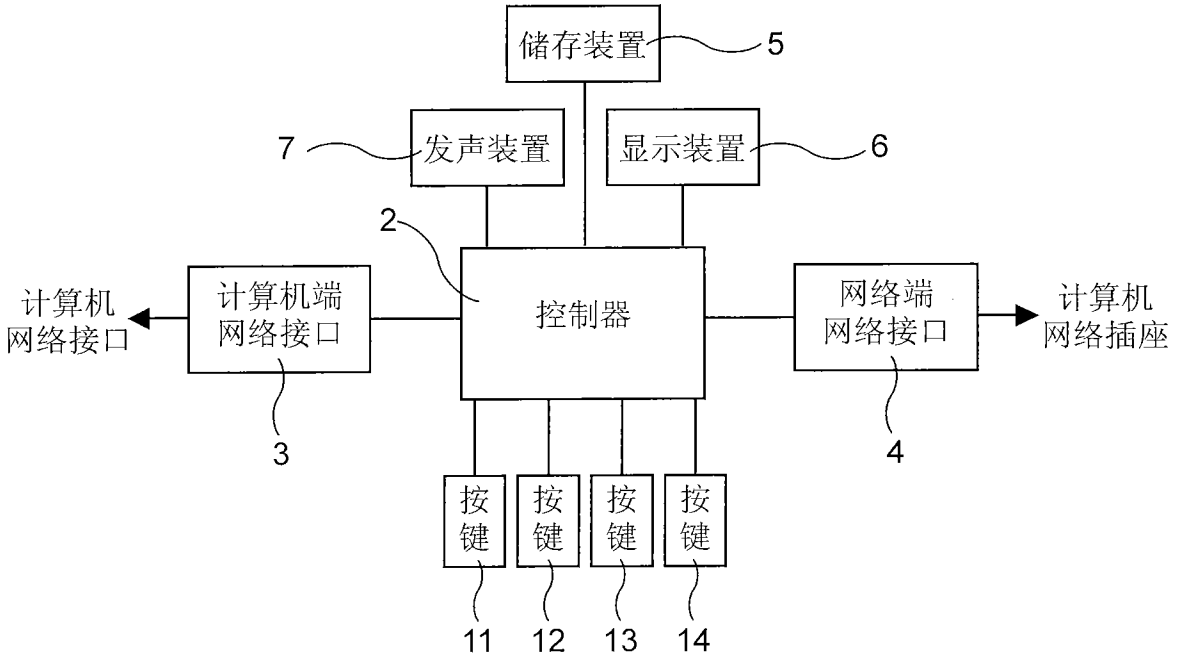

储存装置
5
7
发声装置
显示装置
6
2
计算机
网络接口
计算机端
网络接口
控制器
网络端
网络接口
计算机
网络插座
3
4
按键
按键
按键
按键
11
12
13
14

图 2