

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04Q 7/32 (2006.01)

H04Q 7/38 (2006.01)



# [12] 发明专利申请公布说明书

[21] 申请号 200810133098.2

[43] 公开日 2008年12月3日

[11] 公开号 CN 101316424A

[22] 申请日 2008.7.8

[21] 申请号 200810133098.2

[71] 申请人 阿里巴巴集团控股有限公司

地址 英属开曼群岛大开曼岛

[72] 发明人 程立 李磊

[74] 专利代理机构 北京同达信恒知识产权代理有限公司

代理人 魏杉

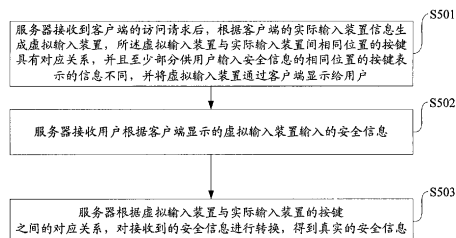
权利要求书 3 页 说明书 8 页 附图 4 页

## [54] 发明名称

一种信息传输方法、系统及装置

## [57] 摘要

本发明公开了一种信息传输方法、系统及装置，用以解决现有技术中存在信息传输的安全性较差的问题。本发明提供的一种信息传输方法包括：服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；所述服务器将所述虚拟输入装置通过所述客户端显示给用户，并接收用户根据所述客户端显示的虚拟输入装置输入的安全信息；所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息。本发明用于在客户端与服务器之间传输信息。



1、一种信息传输方法，其特征在于，该方法包括：

服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；

所述服务器将所述虚拟输入装置通过所述客户端显示给用户，并接收用户根据所述客户端显示的虚拟输入装置输入的安全信息；

所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息。

2、根据权利要求1所述的方法，其特征在于，所述服务器得到所述客户端的实际输入装置信息的步骤包括：

当服务器接收到所述客户端的访问请求后，所述服务器从所述客户端接收到客户端信息；所述服务器通过所述客户端信息，查找到所述客户端的实际输入装置信息。

3、根据权利要求2所述的方法，其特征在于，所述客户端信息为所述客户端的型号。

4、根据权利要求1所述的方法，其特征在于，所述服务器生成所述虚拟输入装置后，还生成该虚拟输入装置的标识。

5、根据权利要求4所述的方法，其特征在于，所述服务器将所述虚拟输入装置通过所述客户端显示给用户的步骤包括：

所述服务器将所述虚拟输入装置输出到所述客户端显示的网页上；并且，将所述虚拟输入装置的标识作为隐藏字段输出到该网页的表单上。

6、根据权利要求5所述的方法，其特征在于，所述服务器接收到通过所述虚拟输入装置输入的安全信息的同时，还接收到该虚拟输入装置的标识，并根据该标识查找到所述对应关系。

7、根据权利要求1所述的方法，其特征在于，所述实际输入装置信息为所述实际输入装置的各个位置的按键所表示的信息。

8、一种信息传输方法，其特征在于，该方法包括：

服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；并且，将所述虚拟输入装置通过所述客户端显示给用户；

所述客户端接收用户根据所述虚拟输入装置输入的安全信息，并将该安全信息发送给所述服务器；

所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，将来自所述客户端的安全信息转换成真实的安全信息。

9、一种服务器，其特征在于，所述服务器包括：

虚拟输入装置生成单元，用于接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；

虚拟输入装置输出单元，用于将所述虚拟输入装置通过所述客户端显示给用户；

输入信息转换单元，用于接收所述用户根据所述客户端显示的虚拟输入装置输入的安全信息，并根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息。

10、根据权利要求9所述的服务器，其特征在于，所述服务器还包括：

数据库，用以存储客户端的实际输入装置信息及其对应的客户端型号，其中，所述客户端的实际输入装置信息包括该客户端的实际输入装置的各个位置上的按键所表示的信息；

数据查找单元，用于从所述数据库中查找与当前接收到客户端型号相对应

的实际输入装置信息，并将查找到的实际输入装置信息发送给所述虚拟输入装置生成单元。

11、根据权利要求9所述的服务器，其特征在于，所述虚拟输入装置生成单元，还用于为每个虚拟输入装置生成一个对应的标识；

所述服务器还包括：

虚拟输入装置查找单元，用以根据用户提交的虚拟输入装置的标识，从所述虚拟输入装置生成单元中查找与该标识相对应的虚拟输入装置；

所述输入信息转换单元，根据所述虚拟输入装置查找单元查找到的虚拟输入装置，查找该虚拟输入装置与实际输入装置的按键之间的对应关系。

12、一种信息传输系统，其特征在于，所述系统包括：客户端和服务端；

所述客户端，用于在按照用户指示访问所述服务器时，接收并显示所述服务器发送的虚拟输入装置，所述虚拟输入装置与自身的实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；并且，将用户根据该虚拟输入装置输入的安全信息发送给所述服务器；

所述服务器，用于当所述客户端访问自身时，根据所述客户端的实际输入装置信息生成所述虚拟输入装置，并将所述虚拟输入装置通过所述客户端显示给用户；以及，根据虚拟输入装置与实际输入装置的按键之间的对应关系，将来自所述客户端的安全信息转换成真实的安全信息。

## 一种信息传输方法、系统及装置

### 技术领域

本发明涉及通信技术领域，尤其涉及一种信息传输方法、系统及装置。

### 背景技术

在安全要求比较高的电子商务应用中，为了确保用户输入的密码不被别人捕获，通常会采用两种方式：一种是采用 SSL（Security Socket Layer）加密通道，另一种是在客户端安装加密控件。

其中，SSL 是一种安全保密协议，在浏览器和网页（Web）服务器之间构造安全通道来进行数据传输，SSL 运行在 TCP/IP 层之上、应用层之下，为应用程序提供加密数据通道。SSL 采用了 RC4、MD5 以及 RSA 等加密算法，使用 40 位的密钥，适用于商业信息的加密。

但是，当客户端是手机等移动设备时，以上两种方式都存在一定的局限性，以手机为例，现有手机的智能操作系统有很多种，而无论是 SSL 加密通道，还是加密控件的安装，都需要根据不同的手机操作系统进行设计，因此，必然增加成本。另外，现有很多非智能手机的机器性能上无法满足 SSL 加密通道和安全控件的运行，因此，很多手持移动设备无法实现常见的加密算法，或者无法在浏览器上安装安全控件。

因此，在一些需要对用户密码等信息进行加密传输的高安全要求的商务应用（如：电子支付）中，无法获得可靠的技术保障，这种情况阻碍了电子商务在手机等手持移动设备领域的应用。

综上所述，现有技术中通过无法安装安全控件、无法实现加密算法等功能较弱的移动设备进行信息传输的安全性较差。

## 发明内容

本发明实施例提供了一种信息传输方法、系统及装置，用以解决现有技术中存在的信息传输的安全性较差的问题。

本发明实施例提供的一种信息传输方法包括：

服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；

所述服务器将所述虚拟输入装置通过所述客户端显示给用户，并接收用户根据所述客户端显示的虚拟输入装置输入的安全信息；

所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息。

本发明实施例提供的一种信息传输方法包括：

服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；并且，将所述虚拟输入装置通过所述客户端显示给用户；

所述客户端接收用户根据所述虚拟输入装置输入的安全信息，并将该安全信息发送给所述服务器；

所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，将来自所述客户端的安全信息转换成真实的安全信息。

本发明实施例提供的一种服务器包括：

虚拟输入装置生成单元，用于接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；

虚拟输入装置输出单元，用于将所述虚拟输入装置通过所述客户端显示给用户；

输入信息转换单元，用于接收所述用户根据所述客户端显示的虚拟输入装置输入的安全信息，并根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息。

本发明实施例提供的一种信息传输系统包括：

所述客户端，用于在按照用户指示访问所述服务器时，接收并显示所述服务器发送的虚拟输入装置，所述虚拟输入装置与自身的实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；并且，将用户根据该虚拟输入装置输入的安全信息发送给所述服务器；

所述服务器，用于当所述客户端访问自身时，根据所述客户端的实际输入装置信息生成所述虚拟输入装置，并将所述虚拟输入装置通过所述客户端显示给用户；以及，根据虚拟输入装置与实际输入装置的按键之间的对应关系，将来自所述客户端的安全信息转换成真实的安全信息。

本发明实施例中，服务器接收到客户端的访问请求后，根据所述客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；所述服务器将所述虚拟输入装置通过所述客户端显示给用户，并接收用户根据所述客户端显示的虚拟输入装置输入的安全信息；所述服务器根据虚拟输入装置与实际输入装置的按键之间的对应关系，对接收到的安全信息进行转换，得到真实的安全信息，从而使得安全性要求较高的信息在网路中没有明文传输，因此避免了在客户端无法安装安全加密控件的情况下，避免了信息的明文传输，有效地防止了安全性要求较高的信息被窃取的问题，从而很大程度地提高了信息传输的安全性。

## 附图说明

- 图 1 为本发明实施例提供的一种信息传输系统的结构示意图；  
图 2 为本发明实施例提供的一种手机的实际键盘的按键布局示意图；  
图 3 为本发明实施例提供的一种手机的虚拟键盘的按键布局示意图；  
图 4 为本发明实施例提供的一种服务器的结构示意图；  
图 5 为本发明实施例提供的一种信息传输方法的流程示意图。

## 具体实施方式

本发明实施例提出了一种信息传输方法、系统及装置，用以提高信息传输的安全性。

本发明实施例中所述的客户端一般为功能较弱的客户端，例如，无法安装安全控件、无法实现加密算法的普通手机等移动设备。

本发明实施例以手机为例进行技术方案的说明，则本发明实施例所述的输入装置为手机的键盘。当然，与手机相类似的客户端都可以采用本发明实施例提供的技术方案。

本发明实施例中将用户的帐户密码等需要保密的、安全级别要求较高的信息称为安全信息。

下面结合附图对本发明实施例进行说明。

参见图 1，本发明实施例提供的一种信息传输系统包括：

客户端 10，用于在按照用户指示访问服务器 11 时，接收并显示所述服务器 11 发送的虚拟输入装置，所述虚拟输入装置与自身的实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同；以及，将用户根据该虚拟输入装置输入的安全信息发送给服务器 11。

服务器 11，用于当所述客户端 10 访问自身时，根据所述客户端 10 的实际输入装置信息生成所述虚拟输入装置，并将所述虚拟输入装置通过所述客户端



10 显示给用户；以及，根据虚拟输入装置与实际输入装置的按键之间的对应关系，将所述客户端 10 发送过来的安全信息转换成真实的安全信息。

较佳地，当用户通过客户端 10 访问服务器 11 时，所述服务器 11 从所述客户端 10 接收到客户端信息；所述服务器 11 通过所述客户端信息查找到该信息对应的所述客户端 10 的实际输入装置信息。其中，所述客户端信息为所述客户端 10 的型号，所述实际输入装置信息为所述实际输入装置的各个位置的按键所表示的信息。

较佳地，所述服务器 11 生成虚拟输入装置的同时，还为该虚拟输入装置分配唯一的一个标识。所述服务器 11 将所述虚拟输入装置输出到所述客户端 10 显示的网页上，并且，将所述虚拟输入装置的标识作为隐藏字段输出到该网页的表单上。所述服务器 11 接收到通过所述虚拟输入装置输入的安全信息的同时，还接收到该虚拟输入装置的标识，并根据该标识查找到虚拟输入装置的按键布局与实际输入装置的按键布局之间的对应关系。

需要说明的是，服务器 11 每次接收到客户端 10 的访问请求所生成的虚拟输入装置的按键都是不同的，也可以是周期性地更新生成的虚拟输入装置，即每隔若干次接收到客户端 10 的访问请求，就变更一次所生成的虚拟输入装置。

下面以手机为例给出具体说明。

用户通过手机的浏览器进入请求登录的网页（web 页面），登陆成功后，手机的型号被传送至服务器，该服务器存储有市面上绝大部分手机的硬件信息及其对应的手机型号，其中所述手机的硬件信息包括该手机的键盘的各个位置的按键所表示的信息；该服务器查找与当前接收到的手机型号相对应的手机的键盘布局信息；根据该键盘（实际键盘）信息，随机调换该实际键盘上的按键的位置，生成一个与该实际键盘的按键布局不同的虚拟键盘，保存该虚拟键盘上的按键与实际键盘上的按键之间的对应关系，并为每个虚拟键盘分配唯一的一个标识，以便后续查找该虚拟键盘；将生成的虚拟键盘输出并显示到用户通过手机登录的 web 页面上，同时，将虚拟键盘的标识作为一个隐藏字段输出到

该页面的表单中，即在用户的登录页面的表单中增加一个隐藏字段（这种字段在页面上是不显示的，因此用户看不到）用以保存虚拟键盘标识，当后续用户通过该虚拟键盘输入信息并提交时，会同时提交该虚拟键盘的标识。

其中，生成虚拟键盘的方法包括：把实际键盘上的每个按钮看成一个空格，逐个为每个空格随机填放一个虚拟按键，但是，该虚拟按键与实际按键的位置不同，并且较佳地，不是已经使用过的虚拟按键。

用户按照 web 页面上显示的虚拟键盘的按键位置，在自己的手机上的实际键盘的对应按键位置输入安全信息，并点击提交，此时提交的是虚拟键盘对应的“虚拟”的安全信息，同时提交的还有该虚拟键盘的标识。

服务器根据虚拟键盘的标识，获得保存在该服务器中的与该标识相对应的虚拟键盘，并按照虚拟键盘上的按键与实际键盘上的按键之间的对应关系，将用户通过虚拟键盘输入的“虚拟”的安全信息转换为实际键盘对应的真实的安全信息，转换完成后，对真实的安全信息进行校验等后续工作。

例如，用户真实的帐户密码是 123，用户手机上实际键盘的按键布局如图 2 所示，1、2、3 这三个数字的功能按键在用户手机键盘上位于第三排，并从左向右依次分布，而在服务器随机生成的虚拟键盘的按键布局如图 3 所示，1、2、3 这三个数字的功能按键位于第五排，并从右向左依次分布，那么，用户可以按照该虚拟键盘的按键布局，从右向左依次点击自己手机上的第五排的按键，如图 2 所示，用户手机上的实际键盘第五排从右向左的功能按键依次是 9、8、7，那么手机会将 987 通过网络传输给服务器，而服务器再根据虚拟键盘上的按键布局与实际键盘上的按键布局之间的对应关系，将 987 转换为 123，即得到用户真实的帐户密码，并对该真实的帐户密码进行校验等后续操作。

较佳地，参见图 4，本发明实施例提供的一种服务器包括：

数据库 41，用以存储市面上绝大部分手机的硬件信息及其对应的手机型号，其中，所述手机的硬件信息包括该手机的实际的键盘的各个位置上的按键所表示的信息，例如：该手机的键盘的样式，包括哪些功能按键，每个按键被

点击后可以输入什么样的信息等等。

数据查找单元 42，用以在数据库 41 内查找当前接收到的手机型号所对应的手机的键盘信息。

虚拟输入装置生成单元 43，用以根据数据查找单元 42 查找到的键盘（实际键盘）信息，随机调换该实际键盘上的按键的位置，生成虚拟键盘，所述虚拟键盘与实键盘之间相同位置的按键具有对应关系，并且，至少部分供用户输入安全信息的相同位置的按键表示的信息不同；并保存该虚拟键盘上的按键与实际键盘上的按键之间的对应关系，并为每个虚拟键盘生成唯一对应的一个标识。

虚拟输入装置输出单元 44，用以将虚拟输入装置生成单元 43 生成的虚拟键盘输出并显示到用户通过手机登录的 web 页面上，同时，将该虚拟键盘的标识作为一个隐藏字段输出到该页面的表单中。

虚拟输入装置查找单元 45，用以根据用户提交的虚拟键盘的标识，从虚拟输入装置生成单元 43 中查找到与该标识相对应的虚拟键盘。

输入信息转换单元 46，用以根据虚拟输入装置查找单元 45 查找到的虚拟键盘，从虚拟输入装置生成单元 43 中查找到该虚拟键盘上的按键与实际键盘上的按键之间的对应关系，并根据该对应关系将用户提交的“虚拟”的安全信息转换为实际键盘对应的真实的安全信息。

校验单元 47，用于对真实的安全信息进行校验。

参见图 5，本发明实施例提供的一种信息传输方法包括步骤：

S501、服务器接收到客户端的访问请求后，根据客户端的实际输入装置信息生成虚拟输入装置，所述虚拟输入装置与实际输入装置间相同位置的按键具有对应关系，并且至少部分供用户输入安全信息的相同位置的按键表示的信息不同，并将虚拟输入装置通过客户端显示给用户。

S502、服务器接收用户根据客户端显示的虚拟输入装置输入的安全信息。

S503、服务器根据虚拟输入装置的按键与实际输入装置的按键之间的对应

关系，对接收到的安全信息进行转换，得到真实的安全信息。

综上所述，本发明实施例提供的一种信息传输方案，实现了在功能有限的设备上对用户的安全信息进行“加密”，即客户端发送的是虚拟的安全信息，并非用户真实的安全信息，使得在网络上传输的是虚拟的安全信息，这样就达到了无法在客户端安装加密控件等情况下，避免用户的安全信息明文传输的目的，从而有效地防止了用户的安全信息被窃取，实现了信息的安全传输，并且该方案实现简单、可靠，客户端机器资源占用非常少，易于实现。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

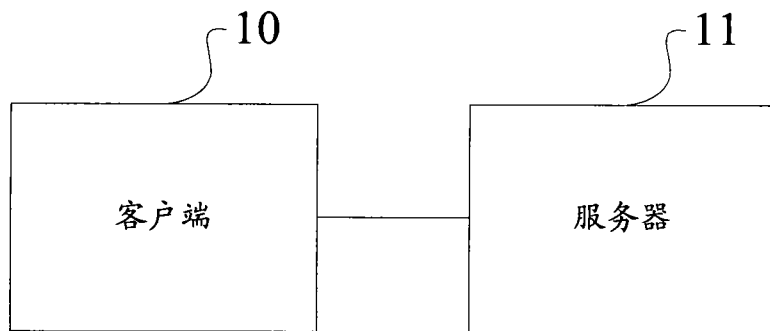


图 1

1	2	3
4	5	6
7	8	9
*	0	#

图 2

9	8	7
0	6	5
3	2	1
*	4	#

图 3

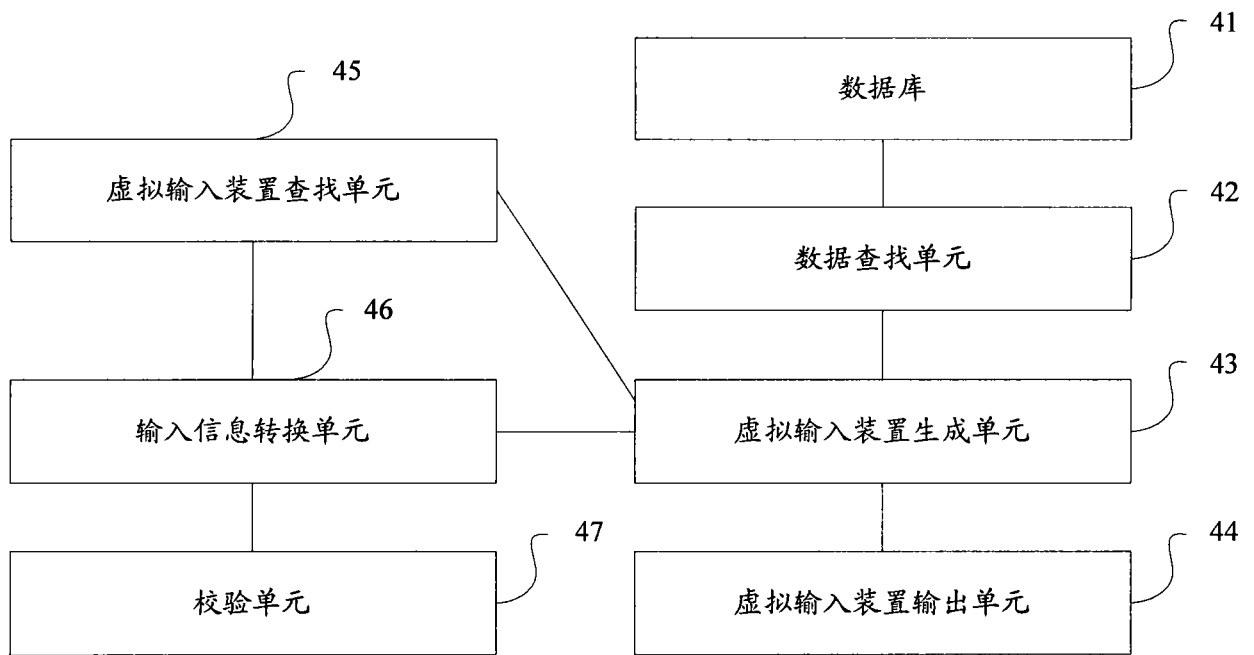


图 4

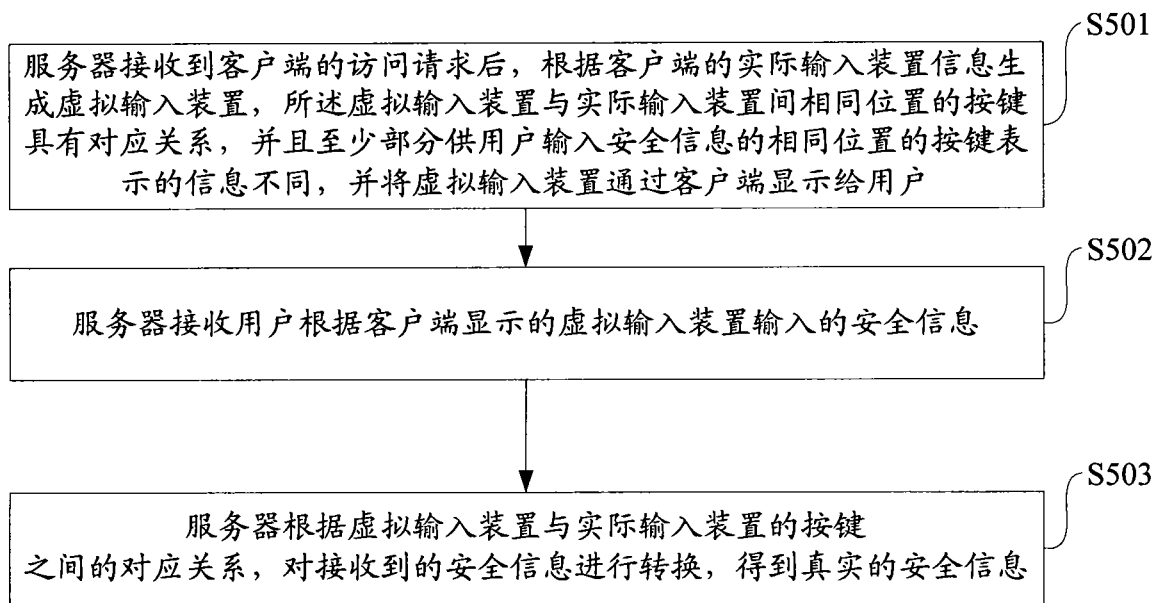


图 5