

一种校验方法及装置

本申请要求 2016 年 08 月 31 日递交的申请号为 201610798104.0、发明名称为“一种校验方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及计算机技术领域，尤其涉及一种校验方法及装置。

背景技术

随着信息技术的发展，网络已成为用户获得业务服务的重要渠道，用户可以在相应的在线系统（如：网站）处使用用户的个人信息获取到相应的在线业务。为了保证在用户获取在线业务过程中的安全性，对用户的身份鉴权也就成为了业务流程中的重要环节（其中，身份鉴权就是对用户个人身份进行校验的过程）。

现有技术中，作为一种常见的身份鉴权方式，安全问题验证得到了广泛应用，尤其是在找回密码的场景下，多数采用安全问题验证的方式实现用户身份的鉴权。具体而言：在线系统自动生成相应的安全问题，并根据用户信息生成匹配该安全问题的正确答案，同时，随机生成若干错误答案。那么，当需要对用户进行安全问题验证时，在线系统会将生成的安全问题以及若干答案选项展示给用户，以完成对用户的身份鉴权。

然而，在线系统自动生成答案选项的过程中，由于采用随机的方式生成错误答案，致使正确答案和错误答案之间的差异性较大，导致非法用户可以较轻易地命中正确答案，从而“冒充”用户通过安全问题的验证。

发明内容

本申请实施例提供一种信息校验方法，用以解决现有技术中安全问题的正确答案和错误答案之间的差异性较大的问题。

25 本申请实施例提供一种校验装置，用以解决现有技术中安全问题的正确答案和错误答案之间的差异性较大的问题。

本申请实施例采用下述技术方案：

本申请实施例提供一种校验方法，包括：

生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案；

30 根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据；

在确定出的各用户数据中，查找与所述用户答案相关的用户数据，作为干扰答案；
根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。

本申请实施例提供的一种校验装置，包括：

安全问题模块，生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的

5 用户答案；

确定模块，根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据；

干扰答案模块，在确定出的各用户数据中，查找与所述用户答案相关的用户数据，作为干扰答案；

10 校验模块，根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。

本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：

业务提供方的服务器在针对用户进行安全问题的身份鉴权的过程中，服务器会生成用于对用户进行校验的安全问题以及与所述安全问题匹配的用户答案（即，正确答案），并基于生成的用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据，确

15 定出的各用户数据均具有与用户答案相同的类别标识信息，换言之，确定出的各用户数据与用户答案的用户数据属于同类型的用户数据，那么，可在确定出的各用户数据中，查找与用户答案相关的用户数据作为干扰答案，显然，干扰答案与用户答案具有相同的类别标识信息，从而使得干扰答案与用户答案之间的差异性较小，也就保证了干扰答案与用户答案较为相似，那么，服务器便可基于安全问题、由用户答案和干扰答案构成的
20 答案选项，对用户进行身份校验。相较于现有技术中的方式而言，本申请中的干扰答案不再是随机生成，而是与用户答案具有相同的类别标识信息，换言之，用户答案与干扰答案属于同一类别，有效提升了干扰答案的干扰作用，进而降低了用户答案被非法用户命中的可能性，提升了安全问题校验的安全性。

25 附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为本申请实施例提供的校验过程示意图；

图 2 为本申请实施例提供的校验装置结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在
5 没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

如前所述，当需要对用户进行身份鉴权时，在线系统会自动生成相应的安全问题，及与该安全问题对应的若干答案选项，以使得用户针对该安全问题的答案选项进行选择，完成身份鉴权，但是，由在线系统生成的若干答案选项中，正确答案和错误答案的差异性较大，也即，错误答案的干扰作用较小，进而导致非法用户较容易通过猜测、推
10 断等方式命中正确答案。

基于此，在本申请实施例中，提供一种基于身份鉴权的信息处理方法，以实现服务器能够生成与正确答案较为相似的干扰答案，从而使得非法用户难以准确辨识出正确答案。

需要说明的是，在本申请实施例中，校验过程可由在线业务提供方后台的服务器实现，其中，在线业务提供方包括但不限于：网站、电信运营商、数据中心等能够提供在线业务的业务提供方。用于实现校验过程的服务器，具体可以是负责安全维护功能服务器，如：在线业务提供方后台的安全中心服务器。这里并不构成对本申请的限定。在后
15 续描述中，将在线系统后台的服务器统一称为：服务器。

以下结合附图，详细说明本申请各实施例提供的技术方案。

20 如图 1 所示，示出了本申请实施中的校验过程，该过程具体包括以下步骤：

S101：生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案。

在本申请实施例中，安全问题通常在触发校验后生成，实际应用中，可由用户触发，也可由服务器自行根据实际应用的需要触发。

具体地，在一种可能的场景中，用户可以主动发送校验请求，此时，所述的校验请求用于触发安全问题的校验过程。作为该场景中的一种方式，安全问题的校验过程可以应用在找回密码的场景下，换言之，当用户点击了相应界面（如：网站的账户登录界面）上的“找回密码”选项后，就需要针对该用户的身份进行校验，所以，用户点击上述选
25 项的操作便可视为发出校验请求，进一步地，可参考图 1，由用户所使用的终端向服务器发出校验请求，则服务器便会接收到用户发送的校验请求。

30 在另一种可能的场景中，服务器可以自行按照相应的校验规则，对用户进行身份校

验，如：按照设定的周期，服务器主动生成安全问题；或者，服务器判定用户的某些操作具有风险时，主动生成安全问题，向用户发起校验。当然，这里并不构成对本申请的限定。

在本申请实施例中，安全问题可来源于预先设定的问题库，也就是说，可预先针对不同的场景、业务使用情况设置不同的问题（当然，该过程可由相应的业务程序设置，这里并不构成对本申请的限定），并存入相应的问题库，故在触发校验后，服务器基于问题库生成针对该用户的安全问题。

在本申请实施例中的上述方式中，可以认为，上述的安全问题对于该用户（或非法用户）而言是不可预测的。

在此基础上，服务器将会确定出用户答案。所述的用户答案，就是相对于该用户而言的正确答案。可以理解，作为本申请实施例中的一种方式，通常基于用户数据确定出用户答案。例如：如果针对该用户生成的安全问题为“您所使用过的昵称是什么？”，那么，则可根据该用户自身的账户数据，从中选出该用户使用过的一个昵称作为与该安全问题相匹配的用户答案。

在一种可能的实际应用场景下，对于用户答案的确定，可以采用答案库的方式，具体可为：根据预先建立的安全问题与答案库的对应关系，确定与生成的所述安全问题相对应的答案库，并根据该答案库中的用户数据生成与该安全问题匹配的用户答案。所述的答案库中存储的用户数据，应理解为存储的是各用户的用户数据。

当然，同一答案库中，可能存储有属于该用户的多个用户数据，那么，在根据答案库中的用户数据生成用户答案的过程中，还可以根据用户数据的使用时间、使用频次等，选择其中一用户数据，用以生成用户答案，具体为：当所述答案库中包含属于同一用户的多个用户数据时，分别确定所述多个用户数据的使用时间，从所述多个用户数据中选择使用时间距当前时间最近的一用户数据，或者，分别确定所述多个用户数据的使用次数，并选择使用次数最多的一用户数据。当然，这里并不构成对本申请的限定。

在本申请实施例中，所述的用户数据，可以是根据用户的业务操作生成的业务数据，如：用户购买过的商品、转账金额等与业务相关的数据；还可以是用户的个人信息数据，如：用户的账户名、姓名、出生日期等数据。这里并不构成对本申请的限定。

S102：根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据。

在本申请实施例中，由于用户答案根据用户数据生成，所以用户答案的类别标识信

息，也就是用户数据的类别标识信息。作为本申请实施例中的一种可行方式，服务器可预先针对各用户的用户数据，生成各用户数据的类别标识信息，并基于类别标识信息，对用户数据进行分类。那么，服务器就可根据用户答案的类别标识信息，确定出具有相同类别标识信息的用户数据。

5 其中，所述类别标识信息包括：至少一种个人信息属性标识和/或至少一种业务属性标识。例如：个人信息属性标识，可以包括：性别标识（如：“男”、“女”等标识）、年龄标识（既可以是某一年龄，也可以是划分的年龄段）、账户标识等等，业务属性标识，可以包括：业务类型标识（如：“转账业务”、“支付业务”等标识）、商品类目标识等。

10 显然，本步骤中根据类别标识信息确定相应的用户数据，是为了从中确定出干扰答案，也即，执行下述步骤 S103。

S103：在确定出的各用户数据中，查找与所述用户答案相关的用户数据，作为干扰答案。

在实际应用中，安全问题的答案选项通常设置为多个，多个答案选项中的非用户答案（即，非正确答案）能够起到干扰的作用，故在本申请实施例中，非用户答案也称为干扰答案。

考虑到实际应用中安全问题的多个答案选项之间的差异性较大，使得非法用户容易从中选择出正确的答案选项冒充用户的身份，因此，本申请实施例中的干扰答案均与用户答案相关。本申请实施例中的所述的相关，可以认为是干扰答案与用户答案在字符长度、答案格式以及答案内容上相似，从而可以起到干扰作用。

20 例如：某用户所使用过的昵称为“xiaoming123”，那么，对于安全问题“您所使用过的昵称是什么？”而言，用户答案就可以为“xiaoming123”，相应的干扰答案可以是诸如“xiaoming-aaa”、“xiao-ming”等。实际上，“xiaoming-aaa”、“xiao-ming”是其他用户的昵称。

25 从该示例可见，干扰答案与用户答案较为相似，从而增加了非法用户的识别难度，进一步降低了用户答案被命中的可能性。

也就是说，干扰答案实质上也是用户数据，并且，作为干扰答案的用户数据，与作为用户答案的用户数据，具有相同的类别标识信息，如上例中，用户答案与干扰答案的类别标识信息均为用户昵称。

30 S104：根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。

服务器在生成了安全问题和相应的答案选项后，便可以针对发出校验请求的用户进行身份鉴权。在一种方式下，服务器可将安全问题及其答案选项发送至用户所使用终端，从而，用户可在相应的页面中查看该安全问题及答案选项，并选择其中的某一答案选项完成身份的鉴权。

- 5 通过上述步骤，业务提供方的服务器在针对用户进行安全问题的身份鉴权的过程中，服务器会生成用于对用户进行校验的安全问题以及与所述安全问题匹配的用户答案（即，正确答案），并基于生成的用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据，确定出的各用户数据均具有与用户答案相同的类别标识信息，换言之，确定出的各用户数据与用户答案的用户数据属于同类型的用户数据，那么，可进一步在
- 10 确定出的各用户数据中，查找与用户答案相关的用户数据作为干扰答案，显然，干扰答案与用户答案具有相同的类别标识信息，从而使得干扰答案与用户答案之间的差异性较小，也就保证了干扰答案与用户答案较为相似，那么，服务器便可基于安全问题、由用户答案和干扰答案构成的答案选项，对用户进行身份校验。相较于现有技术中的方式而言，本申请中的干扰答案不再是随机生成，而是与用户答案具有相同的类别标识信息，
- 15 换言之，用户答案与干扰答案属于同一类别，有效提升了干扰答案的干扰作用，进而降低了用户答案被非法用户命中的可能性，提升了安全问题校验的安全性。

- 正如前述，用户答案和干扰答案均是一种用户数据，为了能够查找与用户答案相关的干扰答案，就需要确定出各用户数据的类别标识信息。具体而言，在生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案之前，上述的方法还可包
- 20 括以下步骤：

步骤一：获取各用户的用户数据；

步骤二：确定获取到的各用户数据的类别标识信息；

步骤三：根据各用户数据的类别标识信息，对各用户数据进行分类，针对分类后的每一类用户数据，生成对应的答案库。

- 25 对于上述过程而言，各用户的用户数据的获取过程，可由服务器中相应的数据获取功能实现，这里并不作具体限定。确定获取到的各用户数据的类别标识信息的过程，可以是服务器基于用户数据的元数据（或用户数据的属性信息），为用户数据赋予相应的类别标识信息，这里并不构成对本申请的限定。

- 根据用户数据的类别标识信息，便可以将用户数据进行分类，如：将账户名数据分
- 30 为一类，将商品数据分为一类等等，进一步就可以将分类后的用户数据创建相应的答案

库。可以理解地，对各用户数据进行分类所基于的类别标识信息，实质上是这一类用户数据的共有类别标识信息，如：上述的账户名数据，也即，这类用户数据均属于账户名，故“账户名”这一类别标识信息是这类用户数据的共有类别标识信息；同样，“商品”这一类别标识信息也是商品数据的共有类别标识信息。

- 5 当然，基于共有类别标识信息所分类后的各用户数据，还可能具有其他类别标识信息，如：按照“商品”这一共有类别标识信息，可将所有的商品数据分为一类，但各商品数据还具有各自的细分类别标识信息，诸如服装、日用品、数码产品等。那么，作为本申请实施例中的一种方式，在创建答案库的过程中，可以按照用户数据的各类别标识信息对用户数据划分成大量不同类的用户数据，再分别生成对应的不同答案库。或者，
- 10 作为另一种方式，针对各用户的用户数据，只按照设定的若干类别标识信息，将用户数据分成若干类，生成对应数量的答案库。至于采用何种方式，具体可以根据实际应用的需要进行选择，这里并不构成对本申请的限定。

- 在此基础上，就可以基于每一类别的答案库的共有类别标识信息，建立与安全问题的对应关系，例如：安全问题为“您使用过的昵称是什么？”，便可将该安全问题与类别标识信息为“昵称”的答案库建立对应关系。
- 15 当然，作为一种可能的方式，还可基于类别标识信息，实时生成安全问题，如：基于类别标识信息“昵称”，生成安全问题“您所使用过的昵称是什么？”。另一种方式中，可基于类别标识信息生成多个安全问题，存储于问题库中。这里并不构成对本申请的限定。

- 20 另外需要说明的是，在实际应用中，随着用户进行相应的业务操作，或新用户的加入，用户数据会不断的产生，那么，作为本申请实施例中的一种可选方式，服务器会动态地获取新产生的用户数据，以使得各答案库中的用户数据保持更新。换言之，获取各用户的用户数据，具体包括：在各用户的用户数据发生变更时，获取变更的用户数据；或，按照设定周期获取各用户的用户数据。基于此，所述方法还包括：根据获取到的用户数据，更新与该用户数据对应的答案库。
- 25 在前述内容的基础上，在校验过程中，服务器便可以自行生成相应的安全问题以及多个答案选项，且在此过程中，无需用户预先编辑相应的答案选项。而在多个答案选项中，用户答案与其他干扰答案之间的相似程度（即，相关），将影响非法用户命中用户答案的可能性（用户答案与干扰答案之间越相似，非法用户命中用户答案的可能性越
- 30

低)。

为了保证干扰答案与用户答案之间相关,干扰答案来源于与安全问题相对应的答案库中。例如:假设某安全问题为“您使用过的昵称是什么?”,显然,对于该安全问题而言,其对应的答案库中所存储的用户数据,应该均是相关的昵称数据(可以是其他用户使用的昵称,也可以是预先生成的昵称数据),这样一来,可保证基于该答案库中生成的干扰答案均属于昵称。那么,在从答案库中确定出用户答案的前提下,服务器便可以在相应的答案库中查找并选定干扰答案。

下面将对服务器查找并选定干扰答案的过程进行详细分析、说明:

在本申请实施例中,服务器查找并选定干扰答案主要分成两种方式,具体地:

10 第一种方式:

安全问题的答案选项(无论是用户答案还是干扰答案)可以认为是一种字符串,该字符串可由文字、数字、符号等构成,那么,干扰答案若要起到较强的干扰作用,也就需要与用户答案在字符的表达上和含义上相类似,换言之,干扰答案在语义上,和/或,字符的表达上与用户答案相类似。

15 例如:假设某安全问题的用户答案为“红色羽绒服”,考虑到在语义上和字符表达上相似,所以,相应的干扰答案可以诸如“绿色羽绒服”、“黄色羽绒服”等等。可见,该示例中的干扰答案与用户答案在语义上均表示羽绒服,同时,在字符的表达上,干扰答案与用户答案均由5个文字所构成,且,均采用“颜色”+“物品”的形式进行表达。也就可以认为,上述的用户答案和干扰答案之间的相似程度较高。

20 所以,在该方式下,服务器从答案库中查找与所述用户答案相关的干扰答案的过程,具体可以包括:确定所述用户答案的语义和/或字符,根据所述用户答案的语义和/或字符,在所述答案库中确定各用户数据与所述用户答案的相似度,根据确定的各相似度,从所述答案库中查找与所述用户答案相关的干扰答案。

该过程中,确定用户答案的语义可采用相应的语义识别算法;此外,对于相似度的确定,可以采用诸如:欧式距离相似度、余弦相似度等相似度算法进行确定,这里并不过多赘述。

第二种方式

30 实际应用中,安全问题通常可分成两类:一类安全问题与用户使用业务服务相关,如:“您本周购买过的商品”、“您购买次数最多的服装品牌”等,显然,这两个安全

问题与用户的购买操作紧密相关。另一类安全问题与用户的个人信息相关，如：“您使用过的账户名”、“您使用过的昵称”等，显然，这两个安全问题与用户的账户信息（账户信息属于用户的个人信息）相关。本申请实施例中，针对上述两类安全问题，采用不同的方式确定相应的干扰答案。

5 针对第一类安全问题：

该类安全问题通常与业务服务相关，对应的答案选项通常是业务服务所对应的业务数据，例如：对于安全问题“您本周购买过的商品”而言，与购物业务相关，那么，该安全问题所对应的答案选项可为“XX 牌洗面奶”、“YY 牌洗发水”等商品名称（商品名称属于一种业务数据）。

10 结合上例可知，为了保证此类安全问题的干扰答案与用户答案之间相关，干扰答案需与用户答案具有相似的业务属性标识。在本申请实施例中的一种可选方式中，业务属性标识体现为业务的类目标识（如：商品类目标识），也就是说，在该方式下，干扰答案与用户答案可具有相同的业务类目标识，当然，业务类目标识是由在线业务提供商预先划分的，这里并不过多赘述。

15 基于此，可以保证用户答案与干扰答案之间相关，例如：假设安全问题为“您购买过的商品”，并假设，某用户购买过洗面奶，那么，服务器将洗面奶确定为用户答案（即，正确答案），在此假设，洗面奶的商品类目标识具体为“面部护理”，从而，服务器会在类别标识信息为“商品”的答案库中，进一步查找出具有“面部护理”这一商品类目标识的用户数据，作为干扰答案。得到的安全问题及其答案选项为：

20 您购买过的商品：

- A、面部保湿水
- B、洗面奶
- C、粉底液
- D、面膜

25 该示例中，B 选项为正确答案（即，用户答案），其余选项为干扰答案。可见，干扰答案与用户答案均具有“面部护理”这一商品类目标识，从而使得干扰答案与用户答案之间相关。

但在某些情况下，上述的答案选项中的正确答案，仍有可能被非法用户命中，具体而言，假设用户为男性，该用户的性别信息被非法用户获知，那么，非法用户便可能根据该性别信息推测出选项 B（这是因为，选项 A、C、D 对应的商品更偏向于女性的面部

30

护理商品)。

所以,在上述内容的基础上,为了进一步增加干扰答案与用户答案之间的相关程度,在从答案库中选定干扰答案的过程中,将考虑相应的个人信息属性标识。

其中,个人信息属性标识可包括:用户的自然属性、以及用户的业务属性。具体而言,用户的自然属性,可以如:姓名、性别、年龄等属性。用户的业务属性,可以如:用户的 IP 地址、用户的位置、用户所偏好的商品、用户的消费等级等。

根据个人信息属性标识,可以对答案库中的数据进行一定程度的再分类,例如:按照用户的性别,可将洗面奶分为男用型洗面奶和女用型洗面奶两类。可见,根据个人信息属性标识,便可以将答案库中数据划分成多种类别。

10 仍沿用上例,假设在针对答案库中的商品数据,增加了以个人信息属性的分类,同时假设,上述用户为男性,那么,服务器在选定干扰答案时,其选择的商品数据将同时具有“面部护理”、“男性”这两种类别标识信息。从而,得到的安全问题及其答案选项为:

您购买过的商品:

- 15 A、洗面奶
 B、剃须泡沫
 C、洁面泥
 D、剃须刀

20 该示例中,选项 A 为用户答案,其余选项为干扰答案。可见,该示例中的答案选项之间的相关性更强,相对于前一示例来说,即使非法用户获知了该用户的性别,由于四个选项中的商品均具有“男性”这一类别标识信息,故非法用户也就更难以选择出正确答案。换言之,在结合了个人信息属性标识的情况下,能够进一步降低非法用户命中正确答案的可能性。

25 针对第二类安全问题:

30 该类安全问题通常与用户的个人信息相关,相应地,该类安全问题的答案选项来源于用户的个人信息,如:用户的账户名、昵称、出生日期、年龄段、用户地址等。对于该类安全问题的答案选项而言,更加偏重于字符表达式,所以,当服务器从相应的答案库中选定干扰答案的过程中,将依据用户答案的字符表达式,选择具有相似字符表达式的干扰答案。

具体而言，可以针对答案库中的数据按照字符类型、结构、长度等进行分类，在确定了用户答案（正确答案）后，进一步选定相应的干扰答案。

例如：假设安全问题为“您使用过的账户名”，服务器确定出进行身份鉴权的用户所使用过的账户名为“xiaoming123”，也即，该账户名就是该安全问题的用户答案。

- 5 从该账户名可知，该账户名中包含英文+数字，所以，服务器从类别标识信息为“账户”的答案库中查找“英文+数字”这一分类的账户名，同时，服务器将在属于该分类的账户名中，进一步查找字符长度相匹配的账户名，且按照英文字符的排序，可以查找到“xiaoming”的英文字符。

- 10 上述内容旨在增强干扰答案与用户答案之间的相似程度，也就可以增强干扰答案的干扰作用。所以，生成的安全问题及其答案选项可以为：

您使用过的账户名：

- A、xiaoming789
B、xiaoming333
C、xiaoming123
15 D、xiaoming666

该示例中，选项 C 为用户答案（正确答案），其余选项为干扰答案。从该示例中可见，该安全问题的答案选项的相似程度较高（即，字符表达式相似），使得非法用户难以命中正确答案。

- 20 至此，结合上述内容，步骤 S104 中，根据所述类别标识信息，查找与所述用户答案相关的用户数据，具体包括：当所述用户答案的类别标识信息为业务属性标识时，根据所述业务属性标识，确定类别标识信息对应的答案库，并在确定出的答案库中，根据所述用户的个人信息属性标识，查找与所述个人信息属性标识对应的用户数据，在查找到的用户数据中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据；或

25 当所述用户答案的类别标识信息为个人信息属性标识时，根据所述个人信息属性标识，确定类别标识信息对应的答案库，并在确定出的答案库中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据。

- 30 与用户答案相关的用户数据，就可以作为干扰答案，而在实际应用中，查找与所述用户答案相关的用户数据，是基于各用户数据与用户答案在语义和/或字符上的相似度。

具体而言，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据，包括：根据所述用户答案的语义和/或字符，确定所述用户答案与各用户数据之间的相似度，根据所述相似度，查找与所述用户答案相关的用户数据。

在本申请实施例中，当服务器针对进行身份鉴权的用户生成了安全问题后，将确定
5 出用户答案，并在此基础上，根据用户答案在相应的答案库中确定与用户答案相似的干扰答案。正是由于干扰答案在数据属性、语义和/或字符上与用户答案相似，那么，干扰答案就可以起到较强的混淆作用，使得非法用户难以从答案选项中命中正确答案。

此外，需要说明的是，最终展示给用户的答案选项通常有数量上的限制（即，设定的数量），如：3~6 个选项等，而服务器从答案库中查找到的干扰答案可能有多个，其
10 数量大于设定的答案选项的数量，那么，在这种情况下，服务器将会从查找到的多个干扰答案中，进一步按照与用户答案的相似程度挑选出指定数量的干扰答案。

换言之，作为本申请实施例中的一种可选方式，查找与所述用户答案相关的用户数据，作为干扰答案，具体包括：若查找到的用户数据的数量大于设定阈值，则按照相似度由高到低的顺序，从查找到的用户数据中选择设定数量的用户数据，作为干扰答案。

15

以上为本申请实施例提供的校验方法，基于同样的思路，本申请实施例还提供一种校验装置。

如图 2 所示，校验装置，设置于业务提供方的服务器侧，该装置包括：

安全问题模块 201，生成用于对用户进行校验的安全问题，以及与所述安全问题匹
20 配的用户答案。

确定模块 202，根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据。

干扰答案模块 203，在确定出的各用户数据中，查找与所述用户答案相关的用户数据，作为干扰答案。

25 校验模块 204，根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。

所述装置还包括：预处理模块 205，获取各用户的用户数据，确定获取到的各用户数据的类别标识信息，根据各用户数据的类别标识信息，对各用户数据进行分类，针对分类后的每一类用户数据，生成与各类别标识信息分别对应的答案库。

其中，所述用户数据包括：根据用户的业务操作生成的业务数据、用户的个人信息
30 数据中的至少一种；所述类别标识信息包括：至少一种个人信息属性标识和/或至少一

种业务属性标识。

所述干扰答案模块 203，当所述用户答案的类别标识信息为业务属性标识时，根据所述业务属性标识，确定类别标识信息对应的答案库，并在确定出的答案库中，根据所述用户的个人信息属性标识，查找与所述个人信息属性标识对应的用户数据，在查找到的用户数据中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据；或

当所述用户答案的类别标识信息为个人信息属性标识时，根据所述个人信息属性标识，确定类别标识信息对应的答案库，并在确定出的答案库中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据。

具体地，所述干扰答案模块 203，根据所述用户答案的语义和/或字符，确定所述用户答案与各用户数据之间的相似度，根据所述相似度，查找与所述用户答案相关的用户数据。

更具体地，所述干扰答案模块 203，若查找到的用户数据的数量大于设定阈值，则按照相似度由高到低的顺序，从查找到的用户数据中选择设定数量的用户数据，作为干扰答案。

另外，所述预处理模块 205，在各用户的用户数据发生变更时，获取变更的用户数据；或按照设定周期获取各用户的用户数据，根据获取到的用户数据，更新与所述用户数据对应的答案库。

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数据处理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数据处理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。

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数据处理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。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，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。

5 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。

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。

10 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
15 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。

20 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过程、方法、商品或者设备不仅包括那些要素，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过程、方法、商品或者设备所固有的要素。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过程、方法、商品或者设备中还存在另外的相同要素。

25 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请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。

30 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权利要求书

1. 一种校验方法，其特征在于，所述方法包括：
- 生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案；
- 根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据；
- 5 在确定出的各用户数据中，查找与所述用户答案相关的用户数据，作为干扰答案；
- 根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。
2. 如权利要求 1 所述的方法，其特征在于，在生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案之前，所述方法还包括：
- 获取各用户的用户数据；
- 10 确定获取到的各用户数据的类别标识信息；
- 根据各用户数据的类别标识信息，对各用户数据进行分类，针对分类后的每一类用户数据，生成与各类别标识信息分别对应的答案库；
- 所述用户数据包括：根据用户的业务操作生成的业务数据、用户的个人信息数据中的至少一种；
- 15 所述类别标识信息包括：至少一种个人信息属性标识和/或至少一种业务属性标识。
3. 如权利要求 2 所述的方法，其特征在于，根据所述类别标识信息，查找与所述用户答案相关的用户数据，具体包括：
- 当所述用户答案的类别标识信息为业务属性标识时，根据所述业务属性标识，确定其对应的答案库，并在确定出的答案库中，根据所述用户的个人信息属性标识，查找与
- 20 所述个人信息属性标识对应的用户数据，在查找到的用户数据中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据；或
- 当所述用户答案的类别标识信息为个人信息属性标识时，根据所述个人信息属性标识，确定其对应的答案库，并在确定出的答案库中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据。
- 25 4. 如权利要求 3 所述的方法，其特征在于，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据，具体包括：
- 根据所述用户答案的语义和/或字符，确定所述用户答案与各用户数据之间的相似度；
- 根据所述相似度，查找与所述用户答案相关的用户数据。
- 30 5. 如权利要求 4 所述的方法，其特征在于，查找与所述用户答案相关的用户数据，

作为干扰答案，具体包括：

若查找到的用户数据的数量大于设定阈值，则按照相似度由高到低的顺序，从查找到的用户数据中选择设定数量的用户数据，作为干扰答案。

6. 如权利要求 2 所述的方法，其特征在于，获取各用户的用户数据，具体包括：
- 5 在各用户的用户数据发生变更时，获取变更的用户数据；或
- 按照设定周期获取各用户的用户数据；
- 所述方法还包括：
- 根据获取到的用户数据，更新与该用户数据对应的答案库。
7. 一种校验装置，其特征在于，包括：
- 10 安全问题模块，生成用于对用户进行校验的安全问题，以及与所述安全问题匹配的用户答案；
- 确定模块，根据所述用户答案的类别标识信息，确定与该类别标识信息对应的各用户数据；
- 干扰答案模块，在确定出的各用户数据中，查找与所述用户答案相关的用户数据，
- 15 作为干扰答案；
- 校验模块，根据所述安全问题、用户答案以及干扰答案，对所述用户进行校验。
8. 如权利要求 7 所述的装置，其特征在于，所述装置还包括：预处理模块，获取各用户的用户数据，确定获取到的各用户数据的类别标识信息，根据各用户数据的类别标识信息，对各用户数据进行分类，针对分类后的每一类用户数据，生成与各类别标识
- 20 信息分别对应的答案库；
- 所述用户数据包括：根据用户的业务操作生成的业务数据、用户的个人信息数据中的至少一种；
- 所述类别标识信息包括：至少一种个人信息属性标识和/或至少一种业务属性标识。
9. 如权利要求 8 所述的装置，其特征在于，所述干扰答案模块，当所述用户答案
- 25 的类别标识信息为业务属性标识时，根据所述业务属性标识，确定其对应的答案库，并在确定出的答案库中，根据所述用户的个人信息属性标识，查找与所述个人信息属性标识对应的用户数据，在查找到的用户数据中，根据所述用户答案的语义和/或字符，查找与所述用户答案相关的用户数据；或
- 当所述用户答案的类别标识信息为个人信息属性标识时，根据所述个人信息属性标
- 30 识，确定其对应的答案库，并在确定出的答案库中，根据所述用户答案的语义和/或字

符，查找与所述用户答案相关的用户数据。

10. 如权利要求 9 所述的装置，其特征在于，所述干扰答案模块，根据所述用户答案的语义和/或字符，确定所述用户答案与各用户数据之间的相似度，根据所述相似度，查找与所述用户答案相关的用户数据。

5 11. 如权利要求 10 所述的装置，其特征在于，所述干扰答案模块，若查找到的用户数据的数量大于设定阈值，则按照相似度由高到低的顺序，从查找到的用户数据中选择设定数量的用户数据，作为干扰答案。

12. 如权利要求 8 所述的装置，其特征在于，所述预处理模块，在各用户的用户数据发生变更时，获取变更的用户数据；或按照设定周期获取各用户的用户数据；

10 根据获取到的用户数据，更新与所述用户数据对应的答案库。