

认证登录系统的方法、装置、设备及存储介质

相关申请的交叉引用

本公开要求于 2024 年 12 月 26 日提交中国专利局的申请号为 2024119317680、名称
5 为“认证登录系统的方法、装置、设备及存储介质”的中国专利申请的优先权，其全部
内容通过引用结合在本公开中。

技术领域

本公开涉及登录认证技术领域，具体而言，涉及一种认证登录系统的方法、装置、
10 设备及存储介质。

背景技术

随着互联网技术的发展，各种智能设备或系统的应用变得越来越普及。智能设备或
系统通常都提供管理员账号，以使用户能够使用管理员账号及其对应的登录口令登录智
能设备或系统的管理程序，实现对智能设备或系统进行管理。

15 基于安全性考虑，智能设备或系统通常会配置为在用户初次登录管理程序后要求该
用户修改登录口令，以防止其他人通过默认口令登录管理程序。

然而在实际应用中，用户常常会忘记自己修改的登录口令，需要找回口令或恢复默
认口令后才能重新登录管理程序。而为了提高设备管理的安全性，找回口令或恢复默认
口令的步骤流程通常设置得非常繁琐，因此用户在忘记登录口令时登录智能设备或系统
20 的便捷性不高。

申请内容

本公开实施例的目的在于提供一种认证登录系统的方法、装置、设备及存储介质，
用以提高用户在忘记登录口令时登录智能设备或系统的便捷性。

本公开实施例提供了一种认证登录系统的方法，包括：

25 响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，
将所述当前登录口令进行加密处理，得到加密信息；

接收所述用户输入的待认证登录口令，基于所述当前登录口令对所述待认证登录口
令进行认证，并根据认证的结果确定是否允许所述用户登录所述目标系统；

其中，所述待认证登录口令通过对所述加密信息进行解析获得。

30 在本公开实施例中，通过在智能设备或系统本地获取当前登录口令并加密，以供用

户将加密信息转发至安全服务器进行解密并获取相应登录口令，从而能够在确保安全性
的前提下，提高用户在忘记登录口令时登录智能设备或系统的便捷性。

在一些可能的实施例中，在接收所述用户输入的待认证登录口令之前，还包括：

基于所述加密信息与预设的请求接口生成请求字符串，以供所述用户基于所述请求
5 字符串将所述加密信息转发至安全服务器，以便所述安全服务器对所述加密信息进行解
析，获得所述待认证登录口令。

在本公开实施例中，通过在智能设备或系统本地预设请求接口并将其结合加密信息
生成用于请求安全服务器的请求字符串，从而进一步提高转发加密信息的效率。

在一些可能的实施例中，所述基于所述加密信息与预设的请求接口生成请求字符串，
10 以供所述用户基于所述请求字符串将所述加密信息转发至所述安全服务器，包括：

基于所述加密信息与预设的请求接口生成请求字符串，并将所述请求字符串转换为
图形识别码，以供所述用户通过所持移动终端扫描所述图形识别码后，基于解析所述图
形识别码得到的请求字符串将所述加密信息转发至所述安全服务器。

在本公开实施例中，通过将请求字符串转换为图形识别码以供移动终端扫码识别并
15 向安全服务器发起请求，从而进一步提高转发加密信息的灵活性。

在一些可能的实施例中，所述加密信息是对所述当前登录口令与所述目标系统的设
备标识进行加密处理得到的；

所述安全服务器被配置为：

接收所述用户转发的加密信息，解析所述加密信息得到对应的当前登录口令和设备
20 标识；

基于预存的注册信息库获取与所述设备标识绑定的注册终端号码，并将所述当前登
录口令发送至与所述注册终端号码对应的目标移动终端。

在本公开实施例中，通过设置注册信息库以实现对不同设备进行登录口令管理，进
一步提高了智能设备登录认证的灵活性。

25 在一些可能的实施例中，所述加密信息是对所述当前登录口令与预设于所述目标系
统中的目标终端号码进行加密处理得到的；

所述安全服务器被配置为：

接收所述用户转发的加密信息，解析所述加密信息得到对应的当前登录口令和目标
终端号码；

将所述当前登录口令发送至与所述目标终端号码对应的目标移动终端。

在本公开实施例中，通过在智能设备或系统本地预存用户（管理员）对应的手机号码，并将该手机号码与当前登录口令一同加密转发至安全服务器，以使安全服务器对加密信息进行解析后直接将当前登录口令反馈至该手机号码对应的移动终端，从而进一步
5 提高了用户在忘记登录口令时登录智能设备或系统的便捷性。

在一些可能的实施例中，所述认证登录系统的方法还包括：

响应于用户针对所述目标系统的账号注册请求，获取所述账号注册请求指定的待注册终端号码，将所述待注册终端号码与所述目标系统的设备标识进行加密处理，得到注册加密信息；

10 所述安全服务器还被配置为：

接收所述用户转发的所述注册加密信息，解析所述注册加密信息得到对应的待注册终端号码和设备标识；

向对应于所述待注册终端号码的移动终端发送认证信息以对所述待注册终端号码进行身份认证，并在所述身份认证成功通过后将所述待注册终端号码和所述设备标识绑定存储至所述注册信息库。
15

在本公开实施例中，通过安全服务器对用户智能设备提交的注册信息进行认证，进一步提高了用户注册登录账号的安全性。

在一些可能的实施例中，所述响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，将所述当前登录口令进行加密处理，得到加密信息，包括：
20

响应于用户针对目标系统的登录口令获取请求，基于所述登录口令获取请求指定的目标账号获取对应于所述目标账号的预设登录口令，作为所述目标系统的当前登录口令；

将所述目标账号和所述当前登录口令进行加密处理，得到加密信息。

在本公开实施例中，通过根据账号获取不同用户此前预设的登录口令作为当前登录口令，从而以找回口令的方式实现智能设备对不同用户的登录认证，进一步提高了用户在忘记登录口令时登录智能设备或系统的便捷性。
25

在一些可能的实施例中，所述响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，包括：

响应于用户针对目标系统的登录口令获取请求，基于预设的随机算法生成随机登录

口令，作为所述目标系统的当前登录口令。

在本公开实施例中，通过将随机生成的登录口令作为当前登录口令，从而以随机口令的形式实现能设备的登录认证，进一步提高了用户在忘记登录口令时登录智能设备或系统的安全性。

5 在一些可能的实施例中，所述认证登录系统的方法还包括：

 在生成所述随机登录口令之后，若在预设的有效时长之内未接收到与所述随机登录口令相一致的待认证登录口令，则重置所述目标系统的当前登录口令。

 在本公开实施例中，通过对随机登录口令配置有效期限，并在超时未认证成功时对当前的随机登录口令进行无效，从而进一步提高了用户在忘记登录口令时登录智能设备
10 或系统的安全性。

 在一些可能的实施例中，所述认证登录系统的方法还包括：

 若基于所述当前登录口令对所述用户输入的待认证登录口令进行认证失败的次数超过预设次数阈值，则对所述用户的登录账号进行锁定。

 在本公开实施例中，通过对连续认证失败超限的用户账号进行锁定，从而进一步提
15 高了用户在忘记登录口令时登录智能设备或系统的安全性。

 在一些可能的实施例中，所述将所述当前登录口令进行加密处理，得到加密信息，包括：

 从预设的多种加密规则中选择出目标加密规则将所述当前登录口令进行加密处理，得到加密信息，并记录所述目标加密规则对应的加密标识；

20 所述基于所述加密信息与预设的请求接口生成请求字符串，以供所述用户基于所述请求字符串将所述加密信息转发至所述安全服务器，具体为：

 基于所述加密信息、所述加密标识和预设的请求接口生成请求字符串，以供所述用户基于所述请求字符串将所述加密信息和所述加密标识转发至所述安全服务器；

 所述安全服务器被配置为：

25 接收所述用户转发的所述加密信息和所述加密标识，基于所述加密标识获取对应的目标解密规则，基于所述目标解密规则解析所述加密信息得到对应的当前登录口令；并将所述当前登录口令反馈至所述用户。

 在本公开实施例中，通过动态选择加密规则对登录口令等信息进行加密处理，从而进一步提高了用户在忘记登录口令时登录智能设备或系统的安全性。

本公开实施例还提供了一种认证登录系统的装置，包括：

 口令加密模块，配置成响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，将所述当前登录口令进行加密处理，得到加密信息；

 登录认证模块，配置成接收所述用户输入的待认证登录口令，基于所述当前登录口令对所述待认证登录口令进行认证，并根据认证的结果确定是否允许所述用户登录所述目标系统；

 其中，所述待认证登录口令通过对所述加密信息进行解析获得。

本公开实施例还提供了一种电子设备，包括存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述处理器执行所述程序时可实现第一方面任一实施例所述的方法。

本公开实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器运行时可实现第一方面任一实施例所述的方法。

本公开实施例还提供了一种计算机程序产品，所述的计算机程序产品包括计算机程序，其中，所述的计算机程序被处理器执行时可实现第一方面任一实施例所述的方法。

附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对本公开实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本公开的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

- 图 1 为本公开实施例提供的一种认证登录系统的方法的流程示意图；
- 图 2 为本公开实施例提供的认证登录系统的方法的交互系统架构图；
- 图 3 为本公开实施例提供的一种认证登录系统的装置的结构示意图；
- 图 4 为本公开实施例提供的一种电子设备的结构示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行描述。

应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。同时，在本公开的描述中，术语“第一”、“第二”等仅用于区分描述，而不能理解为指示或暗示相对

重要性。

如图 1 所示，本公开实施例提供了一种认证登录系统的方法，可以包括步骤：

S1、响应于用户针对目标系统的登录口令获取请求，获取目标系统的当前登录口令，将当前登录口令进行加密处理，得到加密信息。

5 需要说明的是，本公开实施例的认证登录系统的方法可以由智能设备或系统执行。智能设备或系统可以是任意具备一定处理功能的设备或系统，例如智能手环、家用智能电器、物联网设备或网络设备等。目标系统指的是智能设备或系统中的管理程序。

10 可选地，当用户需要登录智能设备或系统的管理程序（目标系统），并且忘记登录口令时，可以向智能设备或系统发起获取登录口令的请求（登录口令获取请求）。示例性地，可以通过智能设备或系统的可视化界面点击忘记口令的按钮以发起登录口令获取请求。

智能设备或系统接收到用户的登录口令获取请求，则从本地获取用于登录目标系统的当前登录口令。其中，当前登录口令可以是此前设置的固定口令或者即时随机生成的口令。

15 然后，将当前登录口令进行加密处理得到加密信息。

其中，加密过程可以采用预先与安全服务器（例如预先配置的云端服务器）协商的对称加密算法或非对称加密算法（公钥和私钥）实现，从而在安全服务器可以通过相应的解密策略对加密信息进行解密。

20 S2、接收用户输入的待认证登录口令，基于当前登录口令对待认证登录口令进行认证，并根据认证的结果确定是否允许用户登录目标系统；

其中，待认证登录口令可以通过对加密信息进行解析获得。

在一种可能实现的方式中，可通过本地的安全解密程序对该加密信息进行解析获得待认证登录口令。

25 在另一种可能实现的方式中，用户可将加密信息转发至安全服务器，由安全服务器解析加密信息从而获得该待认证登录口令。

需要说明的是，智能设备或系统在生成加密信息之后，加密信息可以智能设备或系统的可视化界面展示；可选地，加密信息也可以通过与智能设备或系统连接的 Web 端（例如一台管理主机）展示；然后，用户可以通过某种通信方式（例如手机等移动终端）获取加密信息并将加密信息转发至安全服务器，再由安全服务器解析该加密信息并返回

相应的登录口令。示例性地，加密信息可以是一段字符串，用户可以在移动终端或者 Web 端通过 URL 请求将该字符串发送至安全服务器，以请求安全服务器对该字符串进行解密。

- 5 示例性地，安全服务器可以采用与加密算法对应的解密算法来对加密信息进行解密，得到当前登录口令，然后将当前登录口令反馈至用户。

示例性地，安全服务器可以将解密后的当前登录口令直接通过用户发送加密信息的链路原路返回。

- 10 可选地，加密信息中可以包含设备标识，这样安全服务器在解析加密信息得到当前登录口令和设备标识之后，可以根据设备标识对应的注册终端号码，将当前登录口令反馈至该注册终端号码对应的目标移动终端。

可选地，加密信息中也可以包含目标终端号码，这样安全服务器在解析加密信息得到当前登录口令和目标终端号码之后，可以直接将当前登录口令发送至与该目标终端号码对应的目标移动终端。

- 15 用户若持有与注册终端号码（目标终端号码）对应的目标移动终端，则在目标移动终端获取到安全服务器返回的登录口令之后，可以根据该登录口令向智能设备或系统输入登录口令进行登录认证。此时智能设备或系统接收到用户输入的登录口令（待认证登录口令），基于本地记录的当前登录口令对待认证登录口令进行认证，示例性地，若待认证登录口令与当前登录口令一致，则认证成功，允许用户登录到目标系统；否则认证失败，拒绝用户登录。

- 20 在本公开实施例，通过在智能设备或系统本地获取当前登录口令并加密，以供用户将加密信息转发至安全服务器进行解密并获取相应登录口令，这样不仅确保了登录口令获取的安全性，并且智能设备或系统无需与移动终端和安全服务器建立通信连接，即可实现登录智能设备或系统，从而有效提高了用户在忘记登录口令的情况下登录智能设备或系统的便捷性。

- 25 需要说明的是，由于登录口令在智能设备或系统侧加密、在安全服务器侧解密，在传输过程中则采用密文传输，因此保证了登录口令在传输过程中的安全性。另外，为了增强加解密的可靠性，可以采用公私钥方式实现对登录口令的加解密；可选地，在智能设备或系统侧采用公钥加密、在安全服务器侧采用私钥解密，这样，即使智能设备或系统被破解，只要保证安全服务器侧的私钥不泄露，依然能确保找回登录口令过程中的信

息保密性。

在一些可能的实施例中，在步骤 S2 之前，还可以包括：

S101、基于加密信息与预设的请求接口生成请求字符串，以供用户基于请求字符串将加密信息转发至安全服务器。

5 需要说明的是，用于请求安全服务器的请求字符串，例如 URL (uniform resource locator, 统一资源定位符)，可以在智能设备或系统本地生成。示例性地，可以将加密信息作为 API 参数，并将其与预设的请求接口（与安全服务器的请求 API）结合生成请求字符串；然后，用户可以通过该请求字符串直接向安全服务器发起连接请求并将加密信息转发至安全服务器。

10 示例性地，智能设备和系统可以展示生成的请求字符串，用户在所持有的移动终端手动输入请求字符串（或采用拍照后文字识别等方式）以触发向安全服务器发送请求；或者，智能设备和系统可以通过有线或无线方式（如蓝牙、热点网络等）向用户所持的移动终端发送请求字符串，以使用户所持的移动终端触发向安全服务器发送请求。

基于此，通过在智能设备或系统本地预设请求接口，从而在智能设备或系统本地生成关于加密信息的请求字符串，无需在用户的移动终端处组织生成请求字符串，从而进一步
15 提高转发加密信息的效率和可靠性。

在一些可能的实施例中，步骤 S101，基于加密信息与预设的请求接口生成请求字符串，以供用户基于请求字符串将加密信息转发至安全服务器，可以包括：

S1011、基于加密信息与预设的请求接口生成请求字符串，并将请求字符串转换为
20 图形识别码，以供用户通过所持移动终端扫描图形识别码后，基于解析图形识别码得到的请求字符串将加密信息转发至安全服务器。

可选地，智能设备或系统在本地生成关于加密信息的请求字符串之后，可以进一步将其转换为图形识别码（例如二维码）的形式并展示，由于请求字符串可以是携带加密信息的 URL 字符串，这样，用户可以通过使用移动终端扫描并解析该图形识别码，即可
25 自动连接到该图像识别码对应的 URL，从而直接与安全服务器建立连接并发送加密信息；安全服务器在接收到相应的 API 请求后可以从中获取加密信息并进行解密和反馈登录口令至对应注册号码对应的目标移动终端。

基于此，通过扫码识别请求字符串并自动连接安全服务器和发送加密信息，有效提高了转发加密信息的灵活性，从而有利于进一步提高找回登录口令的便捷性。

在一些可能的实施例中，加密信息是对当前登录口令与目标系统的设备标识进行加密处理得到的；

安全服务器被配置为：

接收用户转发的加密信息，解析加密信息得到对应的当前登录口令和设备标识；

- 5 基于预存的注册信息库获取与设备标识绑定的注册终端号码，并将当前登录口令发送至与注册终端号码对应的目标移动终端。

需要说明的是，在智能设备或系统只支持单用户管理的场景下，设备标识与用户为一一对应的绑定关系，而安全服务器可以通过设备标识实现对不同智能设备或系统进行登录口令的解析和管理。

- 10 可选地，安全服务器在解析用户转发的加密信息，得到相应的当前登录口令和设备标识之后，可以在预存的注册信息库中查找与该设备标识相绑定的注册终端号码，并基于该注册终端号码发送当前登录口令至对应的目标移动终端，在用户所持有的正是该注册终端号码对应的目标移动终端的情况下，则用户可以通过该目标移动终端获取到安全服务器反馈的当前登录口令。其中，注册信息库中存储有不同设备标识及其对应绑定的注册终端号码信息。
- 15

在一些可能的实施例中，在智能设备或系统支持多用户管理的场景下，还可以为同一设备标识注册并绑定多个用户账号。

- 可选地，在注册管理员账号时需要增加用户名（用户账号）的字段，基于此，注册信息库中可以存储有不同设备标识及其对应绑定的不同用户名的注册终端号码信息。
- 20 相应地，在找回登录口令过程中，用户在发起针对目标系统的登录口令获取请求时，需要输入用户名字段，然后智能设备或系统对用户名、设备标识和对应的当前登录口令（与用户名对应）进行加密处理生成加密信息；安全服务器在解密得到用户名、设备标识和对应的当前登录口令之后，首先根据用户名、设备标识在预存的注册信息库中查找相应用户和设备的注册终端号码信息，并基于该注册终端号码发送当前登录口令。
- 25 基于此，通过设置注册信息库对不同设备、不同账号的注册信息进行绑定存储，能够实现对不同设备、不同用户账号进行登录口令管理，从而进一步提高了智能设备登录认证的灵活性。

在一些可能的实施例中，加密信息是对当前登录口令与预设于所述目标系统中的目标终端号码进行加密处理得到的；

安全服务器被配置为：

接收用户转发的加密信息，解析加密信息得到对应的当前登录口令和目标终端号码；
将当前登录口令发送至与目标终端号码对应的目标移动终端。

需要说明的是，在一些可能的实施例中，除了通过对设备标识加密转发至安全服务器并由安全服务器根据解密得到的设备标识确定目标移动终端之外，还可以直接在智能设备或系统本地直接获取预存的管理员对应的目标终端号码，并将目标终端号码与当前登录口令一同进行加密，以供用户将加密信息转发至安全服务器，这样，安全服务器在接收到加密信息并解析之后，可以直接按照目标终端号码将当前登录口令反馈至对应的目标移动终端。

10 其中，智能设备或系统可以在本地预存一个或多个管理员对应的终端号码，在预存有多个管理员对应的终端号码的情况下，用户在发起登录口令获取请求时可以输入用户账号，然后智能设备或系统可以基于用户账号获取对应管理员的目标终端号码，用于与当前登录口令进行加密处理。相应地，当前登录口令可以是随机生成的登录口令，也可以是与用户输入的用户账号对应的预设登录口令。

15 在一些可能的实施例中，认证登录系统的方法还可以包括步骤：

S3、响应于用户针对目标系统的账号注册请求，获取账号注册请求指定的待注册终端号码，将待注册终端号码与目标系统的设备标识进行加密处理，得到注册加密信息；

安全服务器还被配置为：

20 接收用户转发的注册加密信息，解析注册加密信息得到对应的待注册终端号码和设备标识；

向对应于待注册终端号码的移动终端发送认证信息以对待注册终端号码进行身份认证，并在身份认证成功通过后将待注册终端号码和设备标识绑定存储至注册信息库。

需要说明的是，在用户注册账号的过程中，可以设置为类似于步骤 S1 至 S2 的交互流程。可选地，当用户需要注册目标系统的管理员账号时，可以在智能设备或系统发起
25 账号注册请求，并输入想要注册的手机号码（在同一设备支持多用户管理的场景中，还需要输入想要注册的用户名）；然后智能设备或系统根据用户提交的账号注册请求获取该用户输入的待注册终端号码，并将该待注册终端号码与当前智能设备或系统的设备标识进行加密处理，得到注册加密信息。

然后，用户通过某种通信方式（例如通过所持移动终端连接 URL 请求发送）将注

册加密信息转发至安全服务器；示例性地，用户可以通过在移动终端输入注册加密信息的方式，或者使用移动终端扫描二维码（由注册加密信息转换得到）的方式，通过连接 URL 请求将注册加密信息转发至安全服务器。

安全服务器在接收到用户转发的注册加密信息之后，基于智能设备预先确定的加解密协议采用相应的解密算法对注册加密信息进行解密，得到待注册终端号码和设备标识；
5 然后，示例性地安全服务器可以基于待注册终端号码向相应的目标移动终端发送随机验证码，同时基于用户转发注册加密信息的链路原路返回一个输入验证码的验证页面；用户若持有待注册终端号码向相应的目标移动终端，则可以通过目标移动终端接收到随机验证码后在验证页面输入验证码，并将验证码提交至安全服务器；最后安全服务器通过
10 比对用户输入的验证码与此前生成的随机验证码的一致性，以对当前注册用户的身

份进行认证，在认证成功通过后将用户请求注册的待注册终端号码和设备标识绑定存储至注册信息库中。
在一些可能的实施例中，步骤 S1 中，响应于用户针对目标系统的登录口令获取请求，获取目标系统的当前登录口令，将当前登录口令进行加密处理，得到加密信息，可
15 以包括：

S111、响应于用户针对目标系统的登录口令获取请求，基于登录口令获取请求指定的目标账号获取对应于目标账号的预设登录口令，作为目标系统的当前登录口令；

S112、将目标账号和当前登录口令进行加密处理，得到加密信息。

需要说明的是，智能设备或系统在响应用户针对目标系统的登录口令获取请求时，
20 可以采用预先设定并记录的登录口令作为目标系统的当前登录口令。

可选地，在智能设备或系统支持多用户账号共同管理的场景下，不同用户可以针对同一智能设备或系统注册并设置一个相应的登录口令。在忘记口令需要找回时，用户在发起登录口令获取请求时可以输入自己注册的用户名（目标账号），则智能设备或系统可以根据该目标账号获取预先记录的相应预设登录口令作为目标系统的当前登录口令，
25 在经过口令加密以及安全服务器解密口令等流程后，用户可以找回自己此前设置的登录口令并用于登录目标系统。

基于此，通过按照找回口令的方式实现智能设备的登录认证，可以实现多用户账号管理场景的登录认证，进一步提高了用户在忘记登录口令时登录智能设备或系统的便捷性。

在一些可能的实施例中，步骤 S1 中，响应于用户针对目标系统的登录口令获取请求，获取目标系统的当前登录口令，可以包括：

S121、响应于用户针对目标系统的登录口令获取请求，基于预设的随机算法生成随机登录口令，作为目标系统的当前登录口令。

- 5 需要说明的是，在用户忘记口令的情况下，除了找回口令的方式登录目标系统，还可以通过获取随机口令来登录目标系统。

可选地，智能设备或系统在响应用户针对目标系统的登录口令获取请求时，可以基于预设的随机算法生成随机登录口令，作为目标系统的当前登录口令。这样，智能设备或系统无需区分不同的用户账号来找回口令，而是统一采用随机口令的方式实现系统登录认证，进一步提高了用户在忘记登录口令时登录智能设备或系统的便捷性；同时，通过随机生成口令的方式，避免了预设口令被其他用户破解或窃取的情况，从而进一步提高了智能设备或系统登录认证的安全性。

在一些可能的实施例中，认证登录系统的方法还可以包括步骤：

- 15 S4、在生成随机登录口令之后，若在预设的有效时长之内未接收到与随机登录口令相一致的待认证登录口令，则重置目标系统的当前登录口令。

需要说明的是，在采用随机登录口令进行登录认证的场景中，为了进一步提高登录认证的安全性，还可以设置有效登录时限。

- 20 可选地，每次在生成随机登录口令时开始计时，若在预设的有效时长之内未能成功认证登录，也就是在预设的有效时长之内未接收到与当前随机登录口令相一致的待认证登录口令，则重置目标系统的当前登录口令。

其中重置目标系统的当前登录口令，可以是重新生成随机登录口令并采用新的随机登录口令作为当前登录口令，也可以是将目标系统的当前登录口令重置为预设的固定口令。此时，即使用户获取到此前生成的随机登录口令，也无法通过目标系统的认证。用户若想继续找回口令登录系统，则需要重新发起获取登录口令的情况。

- 25 基于此，通过对随机登录口令配置有效期限，并在超时未认证成功时对当前的随机登录口令进行无效，从而进一步提高了智能设备或系统登录认证的安全性。

在一些可能的实施例中，认证登录系统的方法还可以包括步骤：

S5、若基于当前登录口令对用户输入的待认证登录口令进行认证失败的次数超过预设次数阈值，则对用户的登录账号进行锁定。

需要说明的是，为了防止暴力破解，还可以设置登录认证保护策略。可选地，在用户发起找回口令的流程之后，若基于同一个当前登录口令对用户输入的待认证登录口令进行认证失败的次数超过预设的限制次数，则对该用户的登录账号进行锁定。

5 可选地，当锁定该用户的登录账号之后，可以设置为预设的锁定时间，例如三天，在此锁定时间期间内，用户无法再使用该登录账号登录系统。另外，还可以设置应对锁定账户的解锁功能，当锁定用户的登录账号之后，该用户可以通过其他更高级的安全验证方式（例如人工申诉等）请求认证并解锁。

基于此，通过对连续认证失败次数超限的用户账号进行锁定，能够有效防止暴力破解的情况发生，从而进一步提高了智能设备或系统登录认证的安全性。

10 在一些可能的实施例中，步骤 S1 中，将当前登录口令进行加密处理，得到加密信息，可以包括：

从预设的多种加密规则中选择出目标加密规则将当前登录口令进行加密处理，得到加密信息，并记录目标加密规则对应的加密标识；

15 步骤 S101，基于加密信息与预设的请求接口生成请求字符串，以供用户基于请求字符串将加密信息转发至安全服务器，具体为：

基于加密信息、加密标识和预设的请求接口生成请求字符串，以供用户基于请求字符串将加密信息和加密标识转发至安全服务器；

安全服务器被配置为：

20 接收用户转发的加密信息和加密标识，基于加密标识获取对应的目标解密规则，基于目标解密规则解析加密信息得到对应的当前登录口令；并将当前登录口令反馈至用户。

需要说明的是，在每次进行加密处理时也可以从本地预设的多种加密规则（或算法）中选择其中一种，然后由用户将当前使用的加密规则信息（加密标识）与加密信息一同转发至安全服务器，以使安全服务器根据加密标识获取相应的解密规则（或算法）对当前的加密信息进行解密处理。

25 基于此，通过在找回口令的过程中采用不同的加密规则对登录口令等信息进行加密处理，从而进一步提高了用户在忘记登录口令时登录智能设备或系统的安全性。

如图 2 所示，示例性地本公开实施例的认证登录系统的方法主要涉及以下三个部分之间的交互：智能设备或系统、手机和安全服务器。

作为举例，本公开实施例的认证登录系统的方法可以通过以下步骤流程实现：

- 1、响应用户发起的找回口令的请求，智能设备或系统中的程序随机生成一个登录口令，然后将这个登录口令和设备标识（或手机号码）加密处理，得到加密字符串；
- 2、将加密字符串作为 API 参数，将该 API 参数与安全服务器对应的请求 API 组成用于发送给安全服务器的请求 URL 字符串；
- 5 3、将请求 URL 字符串转换为二维码并通过 Web 端展示；
- 4、用户（管理员）使用手机扫描二维码；
- 5、手机扫描二维码后自动连接对应的 URL，将对应的加密字符串传输给安全服务器；
- 6、安全服务器接收到相应的 API 请求之后，从请求中获取加密字符串，然后对其
- 10 解密得到设备标识（或手机号码）和登录口令；
- 7、安全服务器通过可靠的渠道将登录口令通知管理员；例如：根据设备标识获取预先注册登记的手机号码（或直接解析加密字符串得到手机号码），然后发送短信到该手机号码的手机以告知登录口令；或者，在确认管理员身份后口头通知等；
- 8、管理员接收到登录口令后，使用此登录口令登录智能设备或系统；
- 15 9、智能设备或系统接收到管理员输入的登录口令后，将其与此前确定的登录口令进行对比，若对比一致则认证成功并允许该管理员登录系统，否则拒绝登录。

请参考图 3，图 3 示出了本公开的一些实施例提供的认证登录系统的装置的组成框图。应理解，该认证登录系统的装置与上述图 1 方法实施例对应，能够执行上述方法实施例涉及的各个步骤，该认证登录系统的装置的具体功能可以参见上文中的描述，为避免重复，此处适当省略详细描述。

图 3 的认证登录系统的装置包括至少一个能以软件或固件的形式存储于存储器中或固化在认证登录系统的装置中的软件功能模块，该认证登录系统的装置包括：

- 口令加密模块 310，配置成响应于用户针对目标系统的登录口令获取请求，获取目标系统的当前登录口令，将当前登录口令进行加密处理，得到加密信息；
- 25 登录认证模块 320，配置成接收用户输入的待认证登录口令，基于当前登录口令对待认证登录口令进行认证，并根据认证的结果确定是否允许用户登录目标系统；

其中，待认证登录口令是用户将加密信息转发至安全服务器后，由安全服务器解析加密信息并反馈得到的。

可以理解的是上述装置项实施例，是与本公开方法项实施例相对应的，本公开实施

例提供的一种认证登录系统的装置，可以实现本公开任意一项方法项实施例提供的认证登录系统的方法。

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，上述描述的装置的具体工作过程，可以参考前述方法中的对应过程，在此不再过多赘述。

5 如图 4 所示，本公开的一些实施例提供一种电子设备 400，该电子设备 400 包括：存储器 410、处理器 420 以及存储在存储器 410 上并可在处理器 420 上运行的计算机程序，其中，处理器 420 通过总线 430 从存储器 410 读取程序并执行所述程序时可实现如上述认证登录系统的方法包括的任意实施例的方法。

10 处理器 420 可以处理数字信号，可以包括各种计算结构。例如复杂指令集计算机结构、结构精简指令集计算机结构或者一种实行多种指令集组合的结构。在一些示例中，处理器 420 可以是微处理器。

存储器 410 可以配置成存储由处理器 420 执行的指令或指令执行过程中相关的数据。这些指令和/或数据可以包括代码，配置成实现本公开实施例描述的一个或多个模块的一些功能或者全部功能。本公开实施例的处理器 420 可以配置成执行存储器 410 中的指令
15 以实现上述所示的方法。存储器 410 包括动态随机存取存储器、静态随机存取存储器、闪存、光存储器或其它本领域技术人员所熟知的存储器。

本公开的一些实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行方法实施例所述的方法。

20 本公开的一些实施例还提供一种计算机程序产品，所述计算机程序产品在计算机上运行时，使得计算机执行方法实施例所述的方法。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

25 本公开所提供的几个实施例中，应该理解到，所揭露的装置和方法，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的流程图和框图显示了根据本公开的多个实施例的装置、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑

功能的可执行指令。也应当注意，在有些作为替换的实现方式中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

另外，在本公开各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本公开的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本公开各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述仅为本公开的实施例而已，并不用于限制本公开的保护范围，对于本领域的技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

以上所述，仅为本公开的具体实施方式，但本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以所述权利要求的保护范围为准。

需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物品或者设备不仅包

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、物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、物品或者设备中还存在另外的相同要素。

5 工业实用性

本公开实施例提供一种认证登录系统的方法、装置、设备及存储介质，能够在确保安全性的前提下，提高用户在忘记登录口令时登录智能设备或系统的便捷性。

权利要求书

1、一种认证登录系统的方法，其特征在于，包括：

响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，

5 将所述当前登录口令进行加密处理，得到加密信息；

接收所述用户输入的待认证登录口令，基于所述当前登录口令对所述待认证登录口令进行认证，并根据认证的结果确定是否允许所述用户登录所述目标系统；

其中，所述待认证登录口令通过对所述加密信息进行解析获得。

2、根据权利要求 1 所述的认证登录系统的方法，其特征在于，在接收所述用户输入的待认证登录口令之前，还包括：

基于所述加密信息与预设的请求接口生成请求字符串，以供所述用户基于所述请求字符串将所述加密信息转发至安全服务器，以便所述安全服务器对所述加密信息进行解析，获得所述待认证登录口令。

3、根据权利要求 2 所述的认证登录系统的方法，其特征在于，所述基于所述加密信息与预设的请求接口生成请求字符串，以供所述用户基于所述请求字符串将所述加密信息转发至所述安全服务器，包括：

基于所述加密信息与预设的请求接口生成请求字符串，并将所述请求字符串转换为图形识别码，以供所述用户通过所持移动终端扫描所述图形识别码后，基于解析所述图形识别码得到的请求字符串将所述加密信息转发至所述安全服务器。

4、根据权利要求 2 所述的认证登录系统的方法，其特征在于，所述加密信息是对所述当前登录口令与所述目标系统的设备标识进行加密处理得到的；

所述安全服务器被配置为：

接收所述用户转发的加密信息，解析所述加密信息得到对应的当前登录口令和设备标识；

25 基于预存的注册信息库获取与所述设备标识绑定的注册终端号码，并将所述当前登录口令发送至与所述注册终端号码对应的目标移动终端。

5、根据权利要求 2 所述的认证登录系统的方法，其特征在于，所述加密信息是对所述当前登录口令与预设于所述目标系统中的目标终端号码进行加密处理得到的；

所述安全服务器被配置为：

30 接收所述用户转发的加密信息，解析所述加密信息得到对应的当前登录口令和目标

终端号码；

将所述当前登录口令发送至与所述目标终端号码对应的目标移动终端。

6、根据权利要求4所述的认证登录系统的方法，其特征在于，还包括：

5 响应于用户针对所述目标系统的账号注册请求，获取所述账号注册请求指定的待注册终端号码，将所述待注册终端号码与所述目标系统的设备标识进行加密处理，得到注册加密信息；

所述安全服务器还被配置为：

接收所述用户转发的所述注册加密信息，解析所述注册加密信息得到对应的待注册终端号码和设备标识；

10 向对应于所述待注册终端号码的移动终端发送认证信息以对所述待注册终端号码进行身份认证，并在所述身份认证成功通过后将所述待注册终端号码和所述设备标识绑定存储至所述注册信息库。

7、根据权利要求1所述的认证登录系统的方法，其特征在于，所述响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，将所述当前登录
15 口令进行加密处理，得到加密信息，包括：

响应于用户针对目标系统的登录口令获取请求，基于所述登录口令获取请求指定的目标账号获取对应于所述目标账号的预设登录口令，作为所述目标系统的当前登录口令；

将所述目标账号和所述当前登录口令进行加密处理，得到加密信息。

8、根据权利要求1所述的认证登录系统的方法，其特征在于，所述响应于用户针对
20 目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，包括：

响应于用户针对目标系统的登录口令获取请求，基于预设的随机算法生成随机登录口令，作为所述目标系统的当前登录口令。

9、根据权利要求8所述的认证登录系统的方法，其特征在于，还包括：

25 在生成所述随机登录口令之后，若在预设的有效时长之内未接收到与所述随机登录口令相一致的待认证登录口令，则重置所述目标系统的当前登录口令。

10、根据权利要求1所述的认证登录系统的方法，其特征在于，还包括：

若基于所述当前登录口令对所述用户输入的待认证登录口令进行认证失败的次数超过预设次数阈值，则对所述用户的登录账号进行锁定。

11、根据权利要求2所述的认证登录系统的方法，其特征在于，所述将所述当前登

录口令进行加密处理，得到加密信息，包括：

从预设的多种加密规则中选择出目标加密规则将所述当前登录口令进行加密处理，得到加密信息，并记录所述目标加密规则对应的加密标识；

所述基于所述加密信息与预设的请求接口生成请求字符串，以供所述用户基于所述

5 请求字符串将所述加密信息转发至所述安全服务器，具体为：

基于所述加密信息、所述加密标识和预设的请求接口生成请求字符串，以供所述用户基于所述请求字符串将所述加密信息和所述加密标识转发至所述安全服务器；

所述安全服务器被配置为：

10 接收所述用户转发的所述加密信息和所述加密标识，基于所述加密标识获取对应的目标解密规则，基于所述目标解密规则解析所述加密信息得到对应的当前登录口令，并将所述当前登录口令反馈至所述用户。

12、一种认证登录系统的装置，其特征在于，包括：

口令加密模块，用于响应于用户针对目标系统的登录口令获取请求，获取所述目标系统的当前登录口令，将所述当前登录口令进行加密处理，得到加密信息；

15 登录认证模块，用于接收所述用户输入的待认证登录口令，基于所述当前登录口令对所述待认证登录口令进行认证，并根据认证的结果确定是否允许所述用户登录所述目标系统；

其中，所述待认证登录口令通过对所述加密信息进行解析获得。

20 13、一种电子设备，其特征在于，包括存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述处理器执行所述程序时可实现权利要求 1-11 任一所述的认证登录系统的方法。

14、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器运行时执行如权利要求 1-11 任一所述的认证登录系统的方法。

25