(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108063748 A
(43)申请公布日 2018.05.22

(21)申请号 201610987445.2

(22)申请日 2016.11.09

(71)申请人 中国移动通信有限公司研究院
地址 100053 北京市宣武区西便门内大街53A
申请人 中国移动通信集团公司

(72)发明人 程宇

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘

(51)Int.Cl.
H04L 29/06(2006.01)

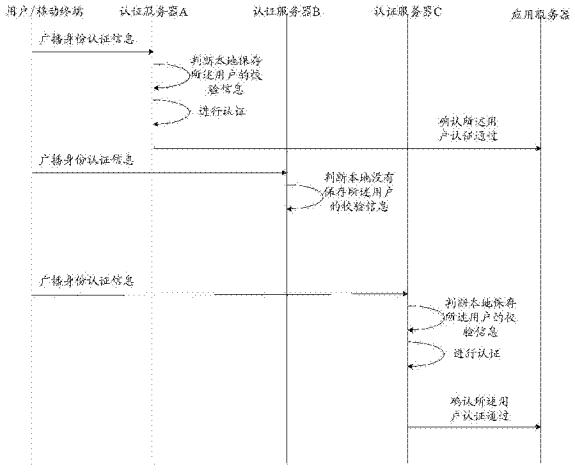
权利要求书4页 说明书20页 附图7页

(54)发明名称

一种用户认证方法、装置及系统

(57)摘要

本发明公开了一种用户认证方法、装置及系统，所述系统包括：应用服务器和至少两个认证服务器；其中，至少两个认证服务器，用于接收用户广播的身份认证信息，根据所述身份认证信息中携带的用户标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；所述应用服务器，用于接收至少两个认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的次数阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。解决了用户并发访问量过大时，集中的认证服务器处理的瓶颈问题。



CN 108063748 A

1.一种用户认证系统，其特征在于，所述用户认证系统包括：应用服务器和至少两个认证服务器；其中，

所述至少两个认证服务器，用于接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；

所述应用服务器，用于接收认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。

2.如权利要求1所述的系统，其特征在于，所述至少两个认证服务器，具体用于接收移动终端广播的私钥加密后的身份认证信息，判断本地是否保存有所述用户的私钥加密后的身份认证信息，如果是，采用针对所述用户保存的公钥，对本地保存的所述用户的私钥加密后的身份认证信息及接收到的所述私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，如果是，确认所述用户认证通过。

3.如权利要求2所述的系统，其特征在于，所述系统还包括：

数字证书服务器，用于接收移动终端发送的注册身份信息，其中所述注册身份信息中携带用户的标识信息，根据所述注册身份信息生成公钥和私钥，将所述公钥和私钥的信息发送给所述移动终端；

所述至少两个认证服务器，还用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息，将所述注册身份信息保存为身份认证信息，并针对所述身份认证信息保存所述公钥。

4.如权利要求3所述的系统，其特征在于，所述至少两个认证服务器，还用于如果判断本地保存有所述用户的校验信息，向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；接收所述数字证书服务器返回的所述用户的公钥的有效期的信息，如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；判断解密后的身份认证信息是否一致；

所述数字证书服务器，还用于接收认证服务器发送的查询公钥的有效期的查询请求，向所述认证服务器返回查询的公钥的有效期的信息。

5.如权利要求3所述的系统，其特征在于，所述数字证书服务器，还用于接收移动终端发送的密钥更新信息，其中所述密钥更新信息中携带用户的标识信息，根据所述密钥更新信息，更新所述用户的公钥和私钥，将更新后的公钥和私钥的信息发送给所述移动终端。

6.如权利要求1所述的系统，其特征在于，所述应用服务器，还用于如果确定所述用户认证通过，根据保存的授权列表，查找所述用户的权限，根据所述用户的权限，向所述用户提供相应服务。

7.如权利要求1所述的系统，其特征在于，所述应用服务器，还用于将所述用户的访问记录广播给认证服务器；

所述至少两个认证服务器，用于接收所述应用服务器广播的用户的访问记录，根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，

针对所述用户保存所述访问记录。

8.一种用户认证方法，其特征在于，应用于权利要求1-7任一项所述的用户认证系统中的认证服务器，所述用户认证系统包括至少两个认证服务器，所述方法包括：

接收移动终端广播的身份认证信息；

根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息；

如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务。

9.如权利要求8所述的方法，其特征在于，所述移动终端广播的身份认证信息为私钥加密后的身份认证信息，所述认证服务器本地保存有私钥加密后的每个身份认证信息；

所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

判断解密后的身份认证信息是否一致。

10.如权利要求9所述的方法，其特征在于，预先保存所述私钥加密后的身份认证信息的过程包括：

接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

11.如权利要求10所述的方法，其特征在于，所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；

接收所述数字证书服务器返回的所述用户的公钥的有效期的信息；

如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

判断解密后的身份认证信息是否一致。

12.如权利要求8所述的方法，其特征在于，所述方法还包括：

接收所述应用服务器广播的用户的访问记录；

根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息；

如果是，针对所述用户保存所述访问记录。

13.一种用户认证方法，其特征在于，应用于权利要求1-7任一项所述的用户认证系统中的应用服务器，所述方法包括：

接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的

标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户认证通过时发送的；

判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；

如果是，确定所述用户认证通过，向所述用户提供相应服务。

14.如权利要求13所述的方法，其特征在于，所述向所述用户提供相应服务包括：

根据保存的授权列表，查找所述用户的权限；

根据所述用户的权限，向所述用户提供相应服务。

15.如权利要求13所述的方法，其特征在于，所述方法还包括：

向认证服务器广播所述用户的访问记录。

16.一种用户认证装置，其特征在于，所述装置包括：

接收模块，用于接收移动终端广播的身份认证信息；

判断模块，用于根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息；如果是，触发认证模块；

认证模块，用于根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，触发发送模块；

发送模块，用于向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务。

17.如权利要求16所述的装置，其特征在于，所述认证模块包括：

解密单元，用于识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

判断单元，用于判断解密后的身份认证信息是否一致。

18.如权利要求17所述的装置，其特征在于，所述装置还包括：

保存模块，用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

19.如权利要求18所述的装置，其特征在于，所述认证模块还包括：

发送单元，用于向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；

接收单元，用于接收所述数字证书服务器返回所述用户的的公钥的有效期的信息；

所述解密单元，还用于如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

所述判断单元，还用于判断解密后的身份认证信息是否一致。

20.如权利要求18所述的装置，其特征在于，所述接收模块，还用于接收所述应用服务器广播的用户的访问记录；

所述判断模块，还用于根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，触发保存模块；

所述保存模块，还用于针对所述用户保存所述访问记录。

21.一种用户认证装置，其特征在于，所述装置包括：

接收模块，用于接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户认证通过时发送的；

判断模块，用于判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；如果是，触发提供服务模块；

提供服务模块，用于确定所述用户认证通过，向所述用户提供相应服务。

22.如权利要求21所述的装置，其特征在于，所述提供服务模块包括：

查找单元，用于根据保存的授权列表，查找所述用户的权限；

提供服务单元，用于根据所述用户的权限，向所述用户提供相应服务。

23.如权利要求21所述的装置，其特征在于，所述装置还包括：

发送模块，用于向认证服务器广播所述用户的访问记录。

一种用户认证方法、装置及系统

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种用户认证方法、装置及系统。

背景技术

[0002] 用户认证功能是目前每个系统中不可缺少的一个功能，目前用户认证功能的实现都是集中在认证服务器中，通过认证服务器来实现用户账号管理、认证管理、授权管理和安全审计，如图1所述，现有技术中用户认证具体为认证服务器接收到用户的身份认证信息后，向账户管理服务器发送查询用户信息，根据账户管理服务器返回的该用户信息查询结果，所述认证服务器确定存在该用户且该用户身份认证通过，并将该用户认证确认信息发送给授权服务器。

[0003] 如图1所示，现有技术该用户认证系统中，认证服务器在接收到用户发送的的身份认证信息时，向账户管理服务器发送查询用户信息，并根据账户管理节点返回的该用户信息查询结果，对该用户进行认证，所有的认证功能都是集中在账户管理服务器和认证服务器中，当用户并发访问量过大时，整个用户认证系统的效率将会受到账户管理服务器和认证服务器的影响，因此用户的访问效率，在很大程度上受到了账户管理服务器和认证服务器瓶颈问题的影响。

发明内容

[0004] 本发明实施例提供了一种用户认证方法、装置及系统，用以解决现有用户的访问效率，在很大程度上受到了账户管理服务器和认证服务器瓶颈问题的影响的问题。

[0005] 为解决上述问题，本发明提供了一种用户认证系统，所述用户认证系统包括：应用服务器和至少两个认证服务器；其中，

[0006] 所述至少两个认证服务器，用于接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；

[0007] 所述应用服务器，用于接收认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0008] 进一步地，所述至少两个认证服务器，具体用于接收移动终端广播的私钥加密后的身份认证信息，判断本地是否保存有所述用户的私钥加密后的身份认证信息，如果是，采用针对所述用户保存的公钥，对本地保存的所述用户的私钥加密后的身份认证信息及接收到的所述私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，如果是，确认所述用户认证通过。

[0009] 进一步地，所述系统还包括：

[0010] 数字证书服务器，用于接收移动终端发送的注册身份信息，其中所述注册身份信

息中携带用户的标识信息，根据所述注册身份信息生成公钥和私钥，将所述公钥和私钥的信息发送给所述移动终端；

[0011] 所述至少两个认证服务器，还用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息，将所述注册身份信息保存为身份认证信息，并针对所述身份认证信息保存所述公钥。

[0012] 进一步地，所述至少两个认证服务器，还用于如果判断本地保存有所述用户的校验信息，向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；接收所述数字证书服务器返回的所述用户的公钥的有效期的信息，如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；判断解密后的身份认证信息是否一致；

[0013] 所述数字证书服务器，还用于接收认证服务器发送的查询公钥的有效期的查询请求，向所述认证服务器返回查询的公钥的有效期的信息。

[0014] 进一步地，所述数字证书服务器，还用于接收移动终端发送的密钥更新信息，其中所述密钥更新信息中携带用户的标识信息，根据所述密钥更新信息，更新所述用户的公钥和私钥，将更新后的公钥和私钥的信息发送给所述移动终端。

[0015] 进一步地，所述应用服务器，还用于如果确定所述用户认证通过，根据保存的授权列表，查找所述用户的权限，根据所述用户的权限，向所述用户提供相应服务。

[0016] 进一步地，所述应用服务器，还用于将所述用户的访问记录广播给认证服务器；

[0017] 所述至少两个认证服务器，用于接收所述应用服务器广播的用户的访问记录，根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，针对所述用户保存所述访问记录。

[0018] 本发明提供了一种一种用户认证方法，应用于所述用户认证系统中的认证服务器，所述用户认证系统包括至少两个认证服务器，所述方法包括：

[0019] 接收移动终端广播的身份认证信息；

[0020] 根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息；

[0021] 如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务。

[0022] 进一步地，所述移动终端广播的身份认证信息为私钥加密后的身份认证信息，所述认证服务器本地保存有私钥加密后的每个身份认证信息；

[0023] 所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

[0024] 识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

[0025] 判断解密后的身份认证信息是否一致。

[0026] 进一步地，预先保存所述私钥加密后的身份认证信息的过程包括：

[0027] 接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信

息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

[0028] 进一步地，所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

[0029] 向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；

[0030] 接收所述数字证书服务器返回的所述用户的公钥的有效期的信息；

[0031] 如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

[0032] 判断解密后的身份认证信息是否一致。

[0033] 进一步地，所述方法还包括：

[0034] 接收所述应用服务器广播的用户的访问记录；

[0035] 根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息；

[0036] 如果是，针对所述用户保存所述访问记录。

[0037] 本发明提供了一种用户认证方法，应用于所述用户认证系统中的应用服务器，所述方法包括：

[0038] 接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户认证通过时发送的；

[0039] 判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；

[0040] 如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0041] 进一步地，所述向所述用户提供相应服务包括：

[0042] 根据保存的授权列表，查找所述用户的权限；

[0043] 根据所述用户的权限，向所述用户提供相应服务。

[0044] 进一步地，所述方法还包括：

[0045] 向认证服务器广播所述用户的访问记录。

[0046] 本发明提供了一种用户认证装置，所述装置包括：

[0047] 接收模块，用于接收移动终端广播的身份认证信息；

[0048] 判断模块，用于根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息；如果是，触发认证模块；

[0049] 认证模块，用于根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，触发发送模块；

[0050] 发送模块，用于向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务。

[0051] 进一步地，所述认证模块包括：

[0052] 解密单元，用于识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

[0053] 判断单元，用于判断解密后的身份认证信息是否一致。

[0054] 进一步地，所述装置还包括：

[0055] 保存模块，用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

[0056] 进一步地，所述认证模块还包括：

[0057] 发送单元，用于向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；

[0058] 接收单元，用于接收所述数字证书服务器返回所述用户的的公钥的有效期的信息；

[0059] 所述解密单元，还用于如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

[0060] 所述判断单元，还用于判断解密后的身份认证信息是否一致。

[0061] 进一步地，所述接收模块，还用于接收所述应用服务器广播的用户的访问记录；

[0062] 所述判断模块，还用于根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，触发保存模块；

[0063] 所述保存模块，还用于针对所述用户保存所述访问记录。

[0064] 本发明提供了一种用户认证装置，所述装置包括：

[0065] 接收模块，用于接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户认证通过时发送的；

[0066] 判断模块，用于判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；如果是，触发提供服务模块；

[0067] 提供服务模块，用于确定所述用户认证通过，向所述用户提供相应服务。

[0068] 进一步地，所述提供服务模块包括：

[0069] 查找单元，用于根据保存的授权列表，查找所述用户的权限；

[0070] 提供服务单元，用于根据所述用户的权限，向所述用户提供相应服务。

[0071] 进一步地，所述装置还包括：

[0072] 发送模块，用于向认证服务器广播所述用户的访问记录。

[0073] 本发明提供了一种用户认证方法、装置及系统，所述系统包括：应用服务器和至少两个认证服务器；其中，所述至少两个认证服务器，用于接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；所述应用服务器，用于接收认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的

数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。由于在本发明的用户认证系统中包括至少两个认证服务器，每个认证服务器保存有对应的用户校验信息，每个认证服务器对对应的用户进行认证，从而有效的降低了每个认证服务器的负担，解决认证服务器处理存在瓶颈的问题，因为存在至少两个认证服务器，应用服务器根据发送认证确认信息的认证服务器的数量，确定用户是否认证通过，从而实现对用户的有效认证。

附图说明

[0074] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，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的附图。

[0075] 图1为现有技术提供的一种用户认证系统的流程示意图；

[0076] 图2为本发明实施例1提供的用户认证系统的认证流程示意图；

[0077] 图3为本发明实施例3提供的用户认证系统的用户注册流程示意图；

[0078] 图4为本发明实施例4提供的用户认证系统的认证流程示意图；

[0079] 图5为本发明实施例7提供的用户认证系统的授权流程示意图；

[0080] 图6为本发明实施例8提供的用户认证方法应用于认证服务器的示意图；

[0081] 图7为本发明实施例13提供的用户认证方法应用于应用服务器的示意图；

[0082] 图8为本发明实施例提供的一种用户认证装置结构图；

[0083] 图9为本发明实施例提供的一种用户认证装置结构图。

具体实施方式

[0084] 为了提高用户的访问效率，解决认证服务器的认证瓶颈问题，本发明实施例提供了一种用户认证方法、装置及系统。

[0085] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明的一部分实施例，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，都属于本发明保护的范围。

[0086] 实施例1：

[0087] 本发明实施例提供了一种用户认证系统，所述系统包括：应用服务器和至少两个认证服务器；其中，

[0088] 至少两个认证服务器，用于接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；

[0089] 所述应用服务器，用于接收认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0090] 为了提高用户的访问效率，解决认证服务器的认证瓶颈问题，在该系统中部署了

至少两个认证服务器，例如认证服务器的数量可以是2个、3个、5个等，每个认证服务器中保存有用户的校验信息，并且该校验信息是针对每个用户进行保存的，其中用户的校验信息可以是用户的注册身份信息，也可以是根据算法生成或加密的包含有用户标识信息的身份信息等。

[0091] 其中每个认证服务器中所保存的用户的校验信息可以完全相同，可以完全不同，也可以部分相同，例如共有5个用户分别为用户A、用户B、用户C、用户D和用户E，包含的认证服务器为3个，分别为认证服务器1、认证服务器2和认证服务器3，其中认证服务器1中保存有用户A、用户B、用户C和用户D的校验信息，认证服务器2中保存有用户A、用户B、用户C和用户E的校验信息，认证服务器3中保存有用户B、用户C、用户D和用户E的校验信息。

[0092] 因为在该用户认证系统中部署了至少两个认证服务器，移动终端为了向每个认证服务器发送身份认证信息，采用广播的方式来广播用户的身份认证信息，其中身份认证信息中携带有用户的标识信息，该用户的标识信息可以是用户的登录账号，也可以是用户的手机号等唯一标识用户的信息。

[0093] 图2为本发明实施例提供的用户认证系统的认证流程示意图，如图2所示，该用户认证系统中包括：认证服务器A、认证服务器B、认证服务器C和应用服务器。

[0094] 用户通过移动终端向该用户认证系统中的认证服务器A、认证服务器B和认证服务器C广播身份认证信息，其中身份认证信息中携带有用户的标识信息，身份认证信息可以为明文的身份认证信息，也可以为经过算法加密后的身份认证信息。认证服务器A、认证服务器B和认证服务器C都可以接收到移动终端广播的身份认证信息。每个认证服务器根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有该用户的校验信息，其中所述用户的校验信息可以为明文的校验信息，也可以为经过算法加密后的身份认证信息。

[0095] 认证服务器B判断本地没有保存所述用户的校验信息，则认证服务器B丢弃接收到的移动终端广播的身份认证信息。

[0096] 认证服务器A和认证服务器C判断本地保存有所述用户的校验信息，根据所述身份认证信息和本地保存的校验信息对所述用户进行认证，如图4所示，认证服务器A和认证服务器C针对所述用户认证通过，向应用服务器发送认证确认信息。

[0097] 所述应用服务器判断针对所述用户，发送认证确认信息的认证服务器的数量已达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务。

[0098] 其中，应用服务器针对不同的用户保存的该数量阈值可以相同，也可以不同，该数量阈值可以根据该用户认证系统中部署的认证服务器的数量，及用户的权限人为进行设定，如果用户的权限较高，则该数量阈值可以较大，该用户认证系统中部署的认证服务器的数量比较多，则该数量阈值也可以比较大。

[0099] 由于本发明实施例提供的用户认证系统中包括至少两个认证服务器，每个认证服务器保存有对应的用户校验信息，每个认证服务器对对应的用户进行认证，从而有效的降低了每个认证服务器的负担，解决认证服务器处理存在瓶颈的问题，因为存在至少两个认证服务器，应用服务器根据发送认证确认信息的认证服务器的数量，确定用户是否认证通过，从而实现对用户的有效认证。

[0100] 实施例2：

[0101] 现有技术中所有用户的认证信息都保存在账户管理节点中，并且是以明文的形式

保存的，如果该账户管理节点被破解，就意味着该用户认证系统中所有用户的认证信息遭到泄露，从而使得用户认证信息的安全性大大降低。为了提高用户身份认证信息的安全性，在上述实施例的基础上，在本发明实施例中，

[0102] 所述至少两个认证服务器，用于接收移动终端广播的私钥加密后的身份认证信息，判断本地是否保存有所述用户的私钥加密后的身份认证信息，如果是，采用针对所述用户保存的公钥，对本地保存的所述用户的私钥加密后的身份认证信息及接收到的所述私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，如果是，确认所述用户认证通过。

[0103] 在本发明实施例中，每个认证服务器保存有大量的用户的校验信息，每条校验信息中包含该用户的标识信息、私钥加密后的身份认证信息，及对应的公钥。每个认证服务器中保存有大量的用户的校验信息，每个认证服务器中保存的用户的校验信息可以相同，可以不同。

[0104] 还以上述例子进行说明，共有5个用户分别为用户A、用户B、用户C、用户D和用户E，包含的认证服务器为3个，分别为认证服务器1、认证服务器2和认证服务器3，其中认证服务器1中保存有用户A、用户B、用户C和用户D的校验信息，认证服务器2中保存有用户A、用户B、用户C和用户E的校验信息，认证服务器3中保存有用户B、用户C、用户D和用户E的校验信息，该校验信息为私钥加密后的身份认证信息，及身份认证信息对应的私钥。

[0105] 如果用户A通过移动终端广播了私钥加密后的身份认证信息，认证服务器1、认证服务器2和认证服务器3接收移动终端广播的私钥加密后的身份认证信息，其中该私钥加密后的身份认证信息中携带用户A的标识信息，该用户A的标识信息是未加密的，认证服务器1、认证服务器2和认证服务器3根据本地针对用户保存校验信息，认证服务器1和认证服务器2判断本地保存有该用户A的校验信息。认证服务器1和认证服务器2根据本地针对该用户A保存的校验信息，识别该校验信息中的公钥信息，采用该公钥对接收到的移动终端广播的加密后的身份认证信息与本地针对用户A保存的私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，认证服务器1和认证服务器2判断解密后的身份认证信息一致，确认所述用户认证通过，并且，认证服务器1和认证服务器2向应用服务器发送认证确认信息。

[0106] 所述采用公钥对私钥加密后的身份认证信息解密的过程属于现有技术，在本发明实施例中对该过程不做赘述。

[0107] 由于本发明实施例中将身份认证信息分别保存在多个不同的认证服务器上，并且认证服务器中保存的身份认证信息是私钥加密后的身份认证信息，因此即使某一认证服务器被破解，也无法获取到该认证服务器中保存的身份认证信息，即使获取到该认证服务器中保存的身份认证信息，也无法获取到该用户认证系统中全部用户的身份认证信息，在一定程度上，保证了用户认证信息的安全。

[0108] 实施例3：

[0109] 为了提高用户认证信息的安全性，在上述各实施例的基础上，在本发明实施例中，该用户认证系统还包括：

[0110] 数字证书服务器，用于接收移动终端发送的注册身份信息，其中所述注册身份信息中携带用户的标识信息，根据所述注册身份信息生成公钥和私钥，将所述公钥和私钥的

信息发送给所述移动终端；

[0111] 所述至少两个认证服务器，还用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息，将所述注册身份信息保存为身份认证信息，并针对所述身份认证信息保存所述公钥。

[0112] 为了提高用户认证信息的安全性，在该系统中采用私钥和公钥来对用户的信息进行加密和解密。其中公钥和私钥信息由数字证书服务器生成。

[0113] 下面以一个具体的实施例对本发明的上述注册和认证过程进行详细说明，图3为本发明实施例提供的用户认证系统的用户注册流程示意图，如图3所示，该用户认证系统中包括：数字证书服务器、认证服务器A、认证服务器B、认证服务器C和应用服务器。

[0114] 用户通过移动终端向数字证书服务器发送注册身份信息，其中所述注册身份信息中携带用户的标识信息及登录密码信息，所述数字证书服务器根据所述注册身份信息生成公钥和私钥，将所述公钥和私钥的信息发送给所述移动终端。所述注册身份信息可以为明文注册身份信息，也可以为根据预设算法生成的注册身份信息，其中所述预设算法可以为哈希算法，针对不同用户的注册身份信息，数字证书服务器生成的公钥和私钥的信息不同。

[0115] 所述数字证书服务器根据所述注册身份信息生成公钥和私钥的过程属于现有技术，在本发明实施例中对该过程不做赘述。

[0116] 所述移动终端接收数字认证服务器发送的公钥和私钥的信息，向认证服务器广播该公钥和采用私钥加密后的注册身份信息。

[0117] 图3中认证服务器A、认证服务器B和认证服务器C都会接收到所述移动终端广播的公钥及采用所述私钥加密后的注册身份信息，其中，认证服务器A和认证服务器C保存所述用户的校验信息，其中该校验信息中包含所述用户的标识信息，该私钥加密后的注册身份信息及公钥，并且认证服务器A和认证服务器C将所述私钥加密后的注册身份信息作为私钥加密后的身份认证信息保存。

[0118] 具体地，该移动终端广播的公钥及采用所述私钥加密后的注册身份信息每个认证服务器都会接收到，但认证认证服务器是否保存该公钥及采用所述私钥加密后的注册身份信息，是根据自身保存的预设规则进行判断的。如果认证服务器判断该公钥及采用所述私钥加密后的注册身份信息满足自身保存的预设规则，则保存该公钥及采用所述私钥加密后的注册身份信息。其中每个认证服务器中保存的预设规则可以不同，也可以相同。

[0119] 其中，每个认证服务器根据保存的预设规则，判断是否保存该公钥及采用所述私钥加密后的注册身份信息时，可以为根据接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息时间段是否为设定的时间段，判断是否进行保存，也可以为接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息后，判断当前保存的用户的校验信息的条数是否达到设定的条数阈值，判断是否进行保存，还可以是在接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息后，识别进行广播的移动终端的地址，判断该地址是否位于自身允许的地址范围内等。其中所述保存的预设规则可以为单一的预设规则，也可以为多个预设规则的叠加。

[0120] 例如所述设定的时间段为0点到12点，如果接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息时间为8点，满足所述设定的时间段，则该认证服务器可以对保存该公钥及采用所述私钥加密后的注册身份信息，例如所述设定的条数阈值为10000条，

如果当前该认证服务器保存的用户的校验信息的条数为5000条，则该认证服务器可以保存该公钥及采用所述私钥加密后的注册身份信息，例如所述自身允许的地址范围为IP地址(Internet Protocol Address，互联网协议地址)127.16.0.0到172.31.255.255，如果识别进行广播的移动终端的地址为127.16.1.100，满足所述自身允许的地址范围，则该服务器可以保存该公钥及采用所述私钥加密后的注册身份信息。

[0121] 由于本发明实施例中将身份认证信息分别保存在多个不同的认证服务器上，并且认证服务器中保存的身份认证信息是私钥加密后的身份认证信息，因此即使某一认证服务器被破解，也无法获取到该认证服务器中保存的身份认证信息，即使获取到该认证服务器中保存的身份认证信息，也无法获取到该用户认证系统中全部用户的身份认证信息，在一定程度上，保证了用户认证信息的安全。

[0122] 实施例4：

[0123] 为了进一步提高用户身份认证信息的安全性，在上述各实施例的基础上，在本发明实施例中，所述至少两个认证服务器，还用于如果判断本地保存有所述用户的校验信息，向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；接收所述数字证书服务器返回的所述用户的公钥的有效期的信息，如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；判断解密后的身份认证信息是否一致；

[0124] 所述数字证书服务器，还用于接收认证服务器发送的查询公钥的有效期的查询请求，向所述认证服务器返回查询的公钥的有效期的信息。

[0125] 一般地，公钥是对私钥加密后的身份认证信息进行解密，如果公钥状态为超过有效期或者未被激活，就会导致身份认证信息无法正常解密或者身份认证信息遭到泄露，所以，在对所述身份认证信息进行解密之前，需要判断所述认证服务器中保存的公钥是否有效，如果有效，所述认证服务器才对所述身份认证信息进行解密。

[0126] 在上述实施例的基础上，图4所示的用户认证系统除认证服务器A、认证服务器B、认证服务器C和应用服务器外，所述用户认证系统还包括：数字证书服务器。

[0127] 具体地，认证服务器A和认证服务器C判断本地保存有所述用户的校验信息后，向数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；所述数字证书服务器将公钥的有效期的查询结果返回给所述认证服务器A和认证服务器C，所述认证服务器A和认证服务器C根据数字证书服务器返回的查询结果判断所述公钥有效，所述认证服务器A和认证服务器C采用所述公钥对接收到的私钥加密后的所述身份认证信息及本地保存的私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，如果是，确认所述用户认证通过并向应用服务器发送认证确认信息。

[0128] 由于所述至少两个认证服务器判断本地保存的公钥是否有效，如果所述公钥有效，才采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密，保证了用户身份认证信息的安全性也进一步提高了用户身份认证信息的安全性。

[0129] 实施例5：

[0130] 为了提高用户认证系统的的灵活性，在上述各实施例的基础上，在本发明实施例中，所述数字证书服务器，还用于接收移动终端发送的密钥更新信息，其中所述密钥更新信

息中携带用户的标识信息，根据所述密钥更新信息，更新所述移动终端的公钥和私钥信息，将更新后的公钥和私钥信息发送给所述移动终端。

[0131] 一般地，公钥是对私钥加密后的身份认证信息进行解密，如果公钥状态为超过有效期或者未被激活，就会导致身份认证信息无法正常解密或者身份认证信息遭到泄露，所以，在认证服务器中保存的公钥应该是处于有效期的公钥。为了保证认证服务器中的公钥有效，在本发明实施例中用户可以通过移动终端向数字证书服务器发送密钥更新信息。

[0132] 数字证书服务器对密钥进行更新具体为：如果所述数字证书服务器接收到移动终端发送的密钥更新信息，根据所述密钥更新信息中携带的用户的标识信息，重新生成公钥和私钥，并将重新生成的该公钥和私钥的信息发送给所述移动终端。移动终端接收到数字证书服务器发送的公钥和私钥后，将更新后的私钥加密的注册身份信息和更新后的公钥的信息重新广播给所述身份认证系统的所有认证服务器。

[0133] 认证服务器接收到移动终端广播的更新后的私钥加密的注册身份信息和更新后的公钥的信息，判断本地是否保存有该用户的校验信息，如果有，采用该更新后的私钥加密的注册身份信息和更新后的公钥的信息，对本地保存该用户的校验信息中的私钥加密后的身份认证信息和公钥进行更新。

[0134] 由于本发明实施例中数字证书服务器可以对用户的公钥和私钥的信息进行更新，从而提高了用户身份认证系统的灵活性。

[0135] 实施例6：

[0136] 现有技术的用户认证系统中包含有授权节点，该授权节点针对认证通过的用户，确定其权限，并将其权限通知应用服务器，应用服务器根据接收到的权限，为用户提供相应的服务。因此可知，在现有的用户认证系统还需要单独部署授权节点，但是该授权节点只是进行用户权限的确定，这就造成了硬件资源的浪费并增大了运营开支。

[0137] 为了节省硬件资源，在上述各实施例的基础上，本发明实施例提供的用户认证系统中，

[0138] 所述应用服务器，还用于如果确定所述用户认证通过，根据保存的授权列表，查找所述用户的权限，根据所述用户的权限，向所述用户提供相应服务。

[0139] 应用服务器在接收到认证服务器发送的认证确认信息后，针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，则确定所述用户认证通过，根据本地预先保存的授权列表，查找所述用户的权限，根据查找的所述用户的权限，向所述用户提供相应服务。其中，应用服务器针对不同的用户保存的该数量阈值可以相同，也可以不同，该数量阈值可以根据所述用户的权限要求，人为进行设定，如果用户的权限较高，则该数量阈值可以较大。应用服务器根据用户权限的不同，向所述用户提供相应服务也不同，如果用户的权限较高，则可以向用户提供的服务越多。

[0140] 在本发明实施例中将授权功能合并到应用服务器中，使得应用服务器在对所述用户进行授权后，直接向所述用户提供相应服务，省去了授权节点和应用服务器之间的交互时间，既提高了用户的访问速度也使得硬件成本与运营开支降低。

[0141] 实施例7：

[0142] 为了方便用户和管理人员后期进行信息查询，在上述各发明实施例的基础上，本发明实施例中提供的用户认证系统中：

[0143] 所述应用服务器，还用于将所述用户的访问记录广播给认证服务器；

[0144] 所述至少两个认证服务器，用于接收所述应用服务器广播的用户的访问记录，根据所述访问记录中包含的用户标识信息，判断本地是否保存有所述用户的校验信息，如果是，针对所述用户保存所述访问记录。

[0145] 图5为本发明实施例提供的用户认证系统的授权流程示意图，如图5所示，

[0146] 应用服务器接收到认证服务器A和认证服务器C发送的用户的认证确认信息，针对该用户，发送认证确认信息的认证服务器的数量为2台，达到设定的数量阈值2台，则应用服务器确定所述用户认证通过，根据本地保存的授权列表，根据所述用户的权限，向所述用户提供相应服务。用户根据应用服务器提供的服务进行访问。

[0147] 应用服务器记录该用户的访问记录，将所述用户的访问记录广播给认证服务器A、认证服务器B和认证服务器C，三个认证服务器接收到所述应用服务器广播的用户的访问记录后，根据所述访问记录中包含的用户标识信息，判断本地是否保存有所述用户的校验信息。其中应用服务器可以在用户访问的同时发送用户的访问记录，也可以在用户完成所有访问后再发送该用户的访问记录，具体的访问记录的发送时机可以根据需要灵活设定。

[0148] 认证服务器B根据所述访问记录中包含的用户标识信息，判断本地没有保存所述用户的校验信息，则丢弃所述访问记录。

[0149] 认证服务器A和认证服务器C根据所述访问记录中包含的用户标识信息，判断本地保存有所述用户的校验信息，则针对所述用户保存所述访问记录。

[0150] 本发明实施例中将所述用户的访问记录保存在认证服务器中，方便了用户和管理员后期信息查询。并且如果至少两个认证服务器中根据该用户的标识信息，保存有所述用户信息的访问记录，如果某一认证服务器被破解，即使篡改该认证服务器上用户的访问记录，，也无法将每个认证服务器上的用户的访问记录都篡改了，在一定程度上，保证了用户的隐私安全和提高了篡改访问记录的难度。

[0151] 实施例8：

[0152] 本发明实施例提供了一种用户认证方法，应用于上述各实施例中的任一认证服务器，图6为本发明实施例提供的用户认证方法应用于认证服务器的示意图，该方法包括以下步骤：

[0153] S601：接收移动终端广播的身份认证信息.

[0154] 本发明实施例提供的用户认证方法，应用于用户认证系统中的认证服务器，所述用户认证系统包括至少两个认证服务器。

[0155] 因为在该用户认证系统中部署了至少两个认证服务器，移动终端为了向每个认证服务器发送身份认证信息，采用广播的方式来广播用户的身份认证信息，其中身份认证信息中携带有用户的标识信息，该用户的标识信息可以是用户的登录账号，可以是用户的手机号等唯一标识用户的信息。

[0156] S602：根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息；

[0157] 在该用户认证系统中部署了至少两个认证服务器，例如认证服务器的数量可以是2个、3个、5个等，每个认证服务器中保存有用户的校验信息，并且该校验信息是针对每个用户进行保存的，其中用户的校验信息可以是用户的注册身份信息，也可以是根据算法生成

或加密的包含有用户标识信息的身份信息等。

[0158] 其中每个认证服务器中所保存的用户的校验信息可以完全相同，可以完全不同，也可以部分相同。

[0159] S603：如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0160] 每个认证服务器中所保存的用户的校验信息可以完全相同，可以完全不同，也可以部分相同，例如共有5个用户分别为用户A、用户B、用户C、用户D和用户E，包含的认证服务器为3个，分别为认证服务器1、认证服务器2和认证服务器3，其中认证服务器1中保存有用户A、用户B、用户C和用户D的校验信息，认证服务器2中保存有用户A、用户B、用户C和用户E的校验信息，认证服务器3中保存有用户B、用户C、用户D和用户E的校验信息。

[0161] 具体的，在认证服务器中针对每个用户保存有该用户的校验信息，该校验信息中保存该用户的标识信息，及该用户的身份认证信息，当认证服务器接收到移动终端广播的身份认证信息，根据该身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，判断该身份认证信息是否与本地保存该用户的校验信息一致，如果一致，则认证服务器确定该用户认证通过。

[0162] 其中，所述校验信息和身份认证信息可以为明文的信息可以为经过同一算法加密后的信息。其中，应用服务器针对不同的用户保存的该数量阈值可以相同，也可以不同，该数量阈值可以根据该用户认证系统中部署的认证服务器的数量，及用户的权限人为进行设定，如果用户的权限较高，则该数量阈值可以较大，该用户认证系统中部署的认证服务器的数量比较多，则该数量阈值也可以比较大。

[0163] 由于本发明实施例提供的用户认证系统中包括至少两个认证服务器，每个认证服务器保存有对应的用户校验信息，每个认证服务器对对应的用户进行认证，从而有效的降低了每个认证服务器的负担，解决认证服务器处理存在瓶颈的问题，因为存在至少两个认证服务器，应用服务器根据发送认证确认信息的认证服务器的数量，确定用户是否认证通过，从而实现对用户的有效认证。

[0164] 实施例9：

[0165] 现有技术中所有用户的认证信息都保存在账户管理节点中，并且是以明文的形式保存的，如果该账户管理节点被破解，就意味着该用户认证系统中所有的用户认证信息遭到泄露，从而使得用户认证信息的安全性大大降低。为了提高用户身份认证信息的安全性，在上述实施例的基础上，本发明实施例中，

[0166] 所述移动终端广播的身份认证信息为私钥加密后的身份认证信息，所述认证服务器本地保存有私钥加密后的每个身份认证信息；

[0167] 所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

[0168] 识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

[0169] 判断解密后的身份认证信息是否一致。

[0170] 在本发明实施例中，每个认证服务器保存有大量的用户的校验信息，每条校验信

息中包含该用户的标识信息、私钥加密后的身份认证信息，及对应的公钥。每个认证服务器中保存有大量的用户的校验信息，每个认证服务器中保存的用户的校验信息可以相同，可以不同。

[0171] 还以上述例子进行说明，共有5个用户分别为用户A、用户B、用户C、用户D和用户E，包含的认证服务器为3个，分别为认证服务器1、认证服务器2和认证服务器3，其中认证服务器1中保存有用户A、用户B、用户C和用户D的校验信息，认证服务器2中保存有用户A、用户B、用户C和用户E的校验信息，认证服务器3中保存有用户B、用户C、用户D和用户E的校验信息，该校验信息为私钥加密后的身份认证信息，及身份认证信息对应的私钥。

[0172] 如果用户A通过移动终端广播了私钥加密后的身份认证信息，认证服务器1、认证服务器2和认证服务器3接收移动终端广播的私钥加密后的身份认证信息，其中该私钥加密后的身份认证信息中携带用户A的标识信息，该用户A的标识信息是未加密的，认证服务器1、认证服务器2和认证服务器3根据本地针对用户保存校验信息，认证服务器1和认证服务器2判断本地保存有该用户A的校验信息。认证服务器1和认证服务器2根据本地针对该用户A保存的校验信息，识别该校验信息中的公钥信息，采用该公钥对接收到的移动终端广播的加密后的身份认证信息与本地针对用户A保存的私钥加密后的身份认证信息进行解密，判断解密后的身份认证信息是否一致，认证服务器1和认证服务器2判断解密后的身份认证信息一致，确认所述用户认证通过，并且，认证服务器1和认证服务器2向应用服务器发送认证确认信息。

[0173] 所述采用公钥对私钥加密后的身份认证信息解密的过程属于现有技术，在本发明实施例中对该过程不做赘述。

[0174] 由于本发明实施例中将身份认证信息分别保存在多个不同的认证服务器上，并且认证服务器中保存的身份认证信息是私钥加密后的身份认证信息，因此即使某一认证服务器被破解，也无法获取到该认证服务器中保存的身份认证信息，即使获取到该认证服务器中保存的身份认证信息，也无法获取到该用户认证系统中全部用户的身份认证信息，在一定程度上，保证了用户认证信息的安全。

[0175] 实施例10：

[0176] 为了提高用户认证信息的安全性，在上述各实施例的基础上，在本发明实施例中，预先保存所述私钥加密后的身份认证信息的过程包括：

[0177] 接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

[0178] 为了提高用户认证信息的安全性，在该用户认证系统中采用私钥和公钥来对用户的信息进行加密和解密。其中公钥和私钥由数字证书服务器生成。

[0179] 注册过程具体为用户通过移动终端向数字证书服务器发送注册身份信息，其中所述注册身份信息中携带用户的标识信息及登录密码信息，所述数字证书服务器根据所述注册身份信息生成公钥和私钥，将所述公钥和私钥的信息发送给所述移动终端。所述注册身份信息可以为明文注册身份信息，也可以为根据预设算法生成的注册身份信息，其中所述预设算法可以为哈希算法，针对不同用户的注册身份信息，数字证书服务器生成的公钥和

私钥的信息不同。

[0180] 所述数字证书服务器根据所述注册身份信息生成公钥和私钥的过程属于现有技术，在本发明实施例中对该过程不做赘述。

[0181] 所述移动终端接收数字认证服务器发送的公钥和私钥的信息，向认证服务器广播该公钥和采用私钥加密后的注册身份信息。

[0182] 具体地，该移动终端广播的公钥及采用所述私钥加密后的注册身份信息每个认证服务器都会接收到，但认证认证服务器是否保存该公钥及采用所述私钥加密后的注册身份信息，是根据自身保存的预设规则进行判断的。如果认证服务器判断该公钥及采用所述私钥加密后的注册身份信息满足自身保存的预设规则，则保存该公钥及采用所述私钥加密后的注册身份信息。其中每个认证服务器中保存的预设规则可以不同，也可以相同。

[0183] 其中，每个认证服务器根据保存的预设规则，判断是否保存该公钥及采用所述私钥加密后的注册身份信息时，可以为根据接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息时间段是否为设定的时间段，判断是否进行保存，也可以为接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息后，判断当前保存的用户的校验信息的条数是否达到设定的条数阈值，判断是否进行保存，还可以是在接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息后，识别进行广播的移动终端的地址，判断该地址是否位于自身允许的地址范围内等。其中所述保存的预设规则可以为单一的预设规则，也可以为多个预设规则的叠加。

[0184] 例如所述设定的时间段为0点到12点，如果接收到移动终端广播的公钥及采用所述私钥加密后的注册身份信息时间为8点，满足所述设定的时间段，则该认证服务器可以对保存该公钥及采用所述私钥加密后的注册身份信息，例如所述设定的条数阈值为10000条，如果当前该认证服务器保存的用户的校验信息的条数为5000条，则该认证服务器可以保存该公钥及采用所述私钥加密后的注册身份信息，例如所述自身允许的地址范围为IP地址(Internet Protocol Address，互联网协议地址)127.16.0.0到172.31.255.255，如果识别进行广播的移动终端的地址为127.16.1.100，满足所述自身允许的地址范围，则该服务器可以保存该公钥及采用所述私钥加密后的注册身份信息。

[0185] 由于本发明实施例中将身份认证信息分别保存在多个不同的认证服务器上，并且认证服务器中保存的身份认证信息是私钥加密后的身份认证信息，因此即使某一认证服务器被破解，也无法获取到该认证服务器中保存的身份认证信息，即使获取到该认证服务器中保存的身份认证信息，也无法获取到该用户认证系统中全部用户的身份认证信息，在一定程度上，保证了用户认证信息的安全。

[0186] 实施例11：

[0187] 为了进一步提高用户身份认证信息的安全性，在上述各实施例的基础上，在本发明实施例中，所述根据所述校验信息及所述身份认证信息对所述用户进行认证包括：

[0188] 向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述用户的标识信息；

[0189] 接收所述数字证书服务器返回所述用户的的公钥的有效期的信息；

[0190] 如果所述公钥有效，采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

[0191] 判断解密后的身份认证信息及身份认证信息是否一致。

[0192] 一般地，公钥是对私钥加密后的身份认证信息进行解密，如果公钥状态为超过有效期或者未被激活，就会导致身份认证信息无法正常解密或者身份认证信息遭到泄露，所以，在对所述身份认证信息进行解密之前，需要判断所述认证服务器中保存的公钥是否有效，如果有效，所述认证服务器才对所述身份认证信息进行解密。其中采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密的过程为现有技术，在本实施例中不做赘述。

[0193] 由于所述至少两个认证服务器判断本地保存的公钥是否有效，如果所述公钥有效，才采用所述公钥对接收到的私钥加密后的身份认证信息及本地保存的私钥加密后的身份认证信息进行解密，保证了用户身份认证信息的安全性也进一步提高了用户身份认证信息的安全性。

[0194] 实施例12：

[0195] 为了方便用户和管理人员后期进行信息查询，在上述各实施例的基础上，该方法还包括：

[0196] 接收所述应用服务器广播的用户的访问记录；

[0197] 根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息；

[0198] 如果是，针对所述用户保存所述访问记录。

[0199] 图5为本发明实施例提供的用户认证系统的授权流程示意图，如图5所示，

[0200] 应用服务器接收到认证服务器A和认证服务器C发送的用户的认证确认信息，针对该用户，发送认证确认信息的认证服务器的数量为2台，达到设定的数量阈值2台，则应用服务器确定所述用户认证通过，根据本地保存的授权列表，根据所述用户的权限，向所述用户提供相应服务。用户根据应用服务器提供的服务进行访问。

[0201] 应用服务器记录该用户的访问记录，将所述用户的访问记录广播给认证服务器A、认证服务器B和认证服务器C，三个认证服务器接收到所述应用服务器广播的用户的访问记录后，根据所述访问记录中包含的用户标识信息，判断本地是否保存有所述用户的校验信息。其中应用服务器可以在用户访问的同时发送用户的访问记录，也可以在用户完成所有访问后再发送该用户的访问记录，具体的访问记录的发送时机可以根据需要灵活设定。

[0202] 认证服务器B根据所述访问记录中包含的用户标识信息，判断本地没有保存所述用户的校验信息，则丢弃所述访问记录。

[0203] 认证服务器A和认证服务器C根据所述访问记录中包含的用户标识信息，判断本地保存有所述用户的校验信息，则针对所述用户保存所述访问记录。

[0204] 本发明实施例中将所述用户的访问记录保存在认证服务器中，方便了用户和管理员后期信息查询。并且如果至少两个认证服务器中根据该用户的标识信息，保存有所述用户信息的访问记录，如果某一认证服务器被破解，即使篡改该认证服务器上用户的访问记录，，也无法将每个认证服务器上的用户的访问记录都篡改了，在一定程度上，保证了用户的隐私安全和提高了篡改访问记录的难度。

[0205] 实施例13：

[0206] 本发明实施例提供了一种用户认证方法，应用于上述各实施例中的任一应用服务

器，图7为本发明实施例提供的用户认证方法应用于应用服务器的示意图，该方法包括以下步骤：

[0207] S701：接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户进行认证通过时发送的；

[0208] 本发明实施例提供的用户认证方法，应用于用户认证系统中的应用服务器，所述用户认证系统包括应用服务器和至少两个认证服务器。因为在该用户认证系统中部署了至少两个认证服务器，用户通过移动终端为了向每个认证服务器发送身份认证信息，采用广播的方式来广播用户的身份认证信息，其中认证服务器的数量可以是2个、3个、5个等。

[0209] 所述认证服务器根据所述校验信息及所述身份认证信息和本地保存的用户的校验信息对所述用户进行认证，如果认证通过，向应用服务器发送认证确认信息。

[0210] S702：判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；

[0211] 应用服务器针对不同的用户保存的该数量阈值可以相同，也可以不同，该数量阈值可以根据该用户认证系统中部署的认证服务器的数量，及用户的权限人为进行设定，如果用户的权限较高，则该数量阈值可以较大，该用户认证系统中部署的认证服务器的数量比较多，则该数量阈值也可以比较大。

[0212] S703：如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0213] 应用服务器根据用户权限的不同，向所述用户提供相应服务也不同，如果用户的权限较高，则所述应用服务器向用户提供的可访问的应用服务越多。具体的因为移动终端向每人认证服务器广播该身份认证信息，而每个认证服务器进行认证的时长是相差不大的，因此应用服务器可以在接收到某一认证服务器发送的认证确认信息时开始计时，判断在设定时间长度内接收到的发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，则确定用户认证通过，否则，确定该用户认证不通过，并删除针对该用户的认证确认信息。

[0214] 由于本发明实施例提供的用户认证系统中包括至少两个认证服务器，每个认证服务器保存有对应的用户校验信息，每个认证服务器对对应的用户进行认证，从而有效的降低了每个认证服务器的负担，解决认证服务器处理存在瓶颈的问题，因为存在至少两个认证服务器，应用服务器根据发送认证确认信息的认证服务器的数量，确定用户是否认证通过，从而实现对用户的有效认证。

[0215] 实施例14：

[0216] 现有技术的用户认证系统中包含有授权节点，该授权节点针对认证通过的用户，确定其权限，并将其权限通知应用服务器，应用服务器根据接收到的权限，为用户提供相应的服务。因此可知，在现有的用户认证系统还需要单独部署授权节点，但是该授权节点只是进行用户权限的确定，这就造成了硬件资源的浪费并增大了运营开支。

[0217] 为了节省硬件资源，在上述各实施例的基础上，在本发明实施例中，所述向所述用户提供相应服务包括：

[0218] 根据保存的授权列表，查找所述用户的权限；

[0219] 根据所述用户的权限，向所述用户提供相应服务。

[0220] 应用服务器的用户权限及可向用户提供的服务可以人为进行设定，根据用户权限的不同，向所述用户提供相应服务也不同，如果用户的权限较高，则可以向该用户提供的服务越多。

[0221] 应用服务器在接收到认证服务器发送的认证确认信息后，针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，则确定所述用户认证通过，根据本地预先保存的授权列表，查找所述用户的权限，根据查找的所述用户的权限，向所述用户提供相应服务。其中，应用服务器针对不同的用户保存的该数量阈值可以相同，也可以不同，该数量阈值可以根据所述用户的权限要求，人为进行设定，如果用户的权限较高，则该数量阈值可以较大。应用服务器根据用户权限的不同，向所述用户提供相应服务也不同，如果用户的权限较高，则可以向用户提供的服务越多。

[0222] 在本发明实施例中将授权功能合并到应用服务器中，使得应用服务器在对所述用户进行授权后，直接向所述用户提供相应服务，省去了授权节点和应用服务器之间的交互时间，既提高了用户的访问速度也使得硬件成本与运营开支降低。

[0223] 实施例15：

[0224] 为了方便用户和管理人员后期进行信息查询，在上述各发明实施例的基础上，本发明提供的所述方法还包括：

[0225] 向认证服务器广播所述用户的访问记录。

[0226] 应用服务器接收到认证服务器A和认证服务器C发送的用户的认证确认信息，针对该用户，发送认证确认信息的认证服务器的数量为2台，达到设定的数量阈值2台，则应用服务器确定所述用户认证通过，根据本地保存的授权列表，根据所述用户的权限，向所述用户提供相应服务。用户根据应用服务器提供的服务进行访问。

[0227] 应用服务器记录该用户的访问记录，将所述用户的访问记录广播给认证服务器A、认证服务器B和认证服务器C，三个认证服务器接收到所述应用服务器广播的用户的访问记录后，根据所述访问记录中包含的用户标识信息，判断本地是否保存有所述用户的校验信息。其中应用服务器可以在用户访问的同时发送用户的访问记录，也可以在用户完成所有访问后再发送该用户的访问记录，具体的访问记录的发送时机可以根据需要灵活设定。

[0228] 认证服务器B根据所述访问记录中包含的用户标识信息，判断本地没有保存所述用户的校验信息，则丢弃所述访问记录。

[0229] 认证服务器A和认证服务器C根据所述访问记录中包含的用户标识信息，判断本地保存有所述用户的校验信息，则针对所述用户保存所述访问记录。

[0230] 本发明实施例中将所述用户的访问记录保存在认证服务器中，方便了用户和管理员后期信息查询。并且如果至少两个认证服务器中根据该用户的标识信息，保存有所述用户信息的访问记录，如果某一认证服务器被破解，即使篡改该认证服务器上用户的访问记录，，也无法将每个认证服务器上的用户的访问记录都篡改了，在一定程度上，保证了用户的隐私安全和提高了篡改访问记录的难度。

[0231] 图8为本发明实施例提供的应用于认证服务器的用户认证装置结构图，应用于用户认证系统中的认证服务器，所述用户认证系统包括至少两个认证服务器，该装置包括：

[0232] 接收模块81，用于接收移动终端广播的身份认证信息；

[0233] 判断模块82，用于根据所述身份认证信息中携带的用户标识信息，判断本地是否保存有所述用户的校验信息；如果是，触发认证模块；

[0234] 认证模块83，用于根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，触发发送模块；

[0235] 发送模块84，用于向应用服务器发送认证确认信息，使所述应用服务器判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的次数阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。

[0236] 所述认证模块83包括：

[0237] 解密单元833，用于识别所述校验信息中的公钥，采用所述公钥，对本地保存的所述校验信息中的私钥加密后的身份认证信息及接收到的私钥加密后的身份认证信息进行解密；

[0238] 判断单元834，用于判断解密后的身份认证信息是否一致。

[0239] 所述装置还包括：

[0240] 保存模块85，用于接收所述移动终端发送的公钥及采用所述私钥加密后的注册身份信息并保存，其中所述私钥加密后的注册身份信息为所述移动终端向数字证书服务器发送的注册身份信息并接收到数字证书服务器发送的公钥和私钥，采用所述私钥信息将所述注册身份信息加密后发送的。

[0241] 所述认证模块83还包括：

[0242] 发送单元831，用于向所述数字证书服务器发送查询公钥的有效期的查询请求，其中所述查询请求中携带所述查询请求中携带所述用户的标识信息；

[0243] 接收单元832，还用于接收所述数字证书服务器返回所述用户的的公钥的有效期的信息；

[0244] 所述解密单元833，还用于如果所述公钥有效，采用所述公钥对接收到的私钥加密后的所述身份认证信息及本地保存的私钥加密后的身份认证信息进行解密；

[0245] 所述判断单元834，还用于判断解密后的身份认证信息是否一致。

[0246] 所述接收模块81，还用于接收所述应用服务器广播的用户的访问记录；

[0247] 所述判断模块82，还用于根据所述访问记录中包含的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，触发保存模块；

[0248] 所述保存模块85，还用于针对所述用户保存所述访问记录。

[0249] 图9为本发明实施例提供的应用于应用服务器的用户认证装置结构图，该装置包括：

[0250] 接收模块91，用于接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户进认证通过时发送的；

[0251] 判断模块92，用于判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值；如果是，触发提供服务模块；

[0252] 提供服务模块93，用于确定所述用户认证通过，向所述用户提供相应服务。

[0253] 所述提供服务模块93包括：

[0254] 查找单元931，用于根据保存的授权列表，查找所述用户的权限；

[0255] 提供服务单元932，用于根据所述用户的权限，向所述用户提供相应服务。

[0256] 所述装置还包括：

[0257] 发送模块94，还用于向认证服务器广播所述用户的访问记录。

[0258] 本发明提供了一种用户认证方法、装置及系统，所述系统包括：应用服务器和至少两个认证服务器；其中，所述至少两个认证服务器，用于接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地是否保存有所述用户的校验信息，如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证，如果认证通过，向所述应用服务器发送认证确认信息；所述应用服务器，用于接收认证服务器发送的认证确认信息，判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值，如果是，确定所述用户认证通过，向所述用户提供相应服务。由于在本发明的用户认证系统中包括至少两个认证服务器，每个认证服务器保存有对应的用户校验信息，每个认证服务器对对应的用户进行认证，从而有效的降低了每个认证服务器的负担，解决认证服务器处理存在瓶颈的问题，因为存在至少两个认证服务器，应用服务器根据发送认证确认信息的认证服务器的数量，确定用户是否认证通过，从而实现对用户的有效认证。

[0259] 对于系统/装置实施例而言，由于其基本相似于方法实施例，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。

[0260] 本领域内的技术人员应明白，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。

[0261] 本申请是参照根据本申请实施例的方法、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。

[0262] 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。

[0263] 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。

[0264] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0265] 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。

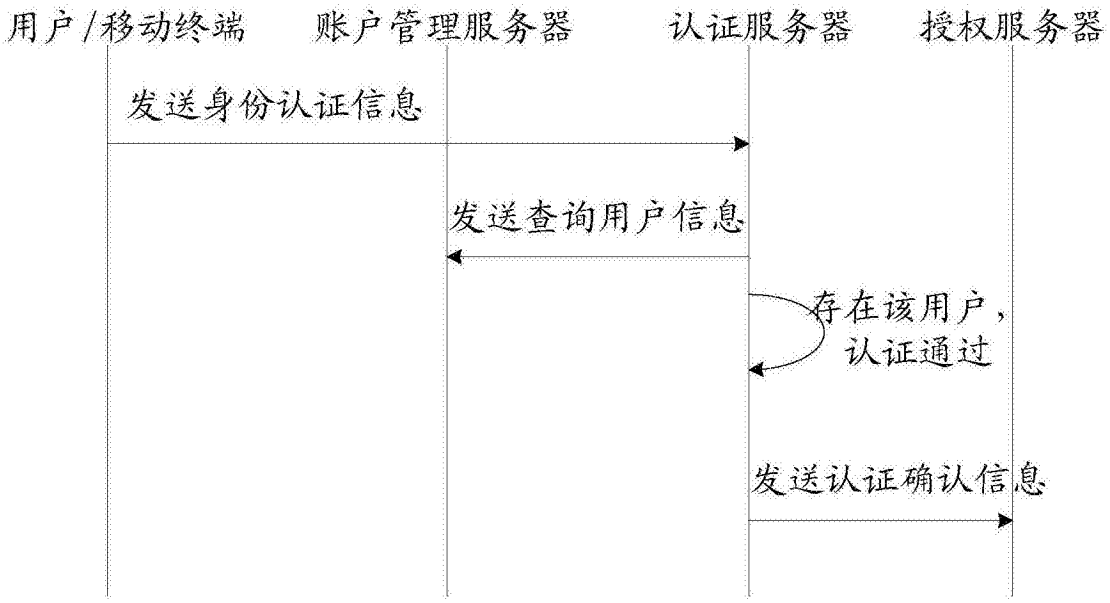

用户/移动终端
账户管理服务器
认证服务器
授权服务器
发送身份认证信息
发送查询用户信息
存在该用户，
认证通过
发送认证确认信息

图1

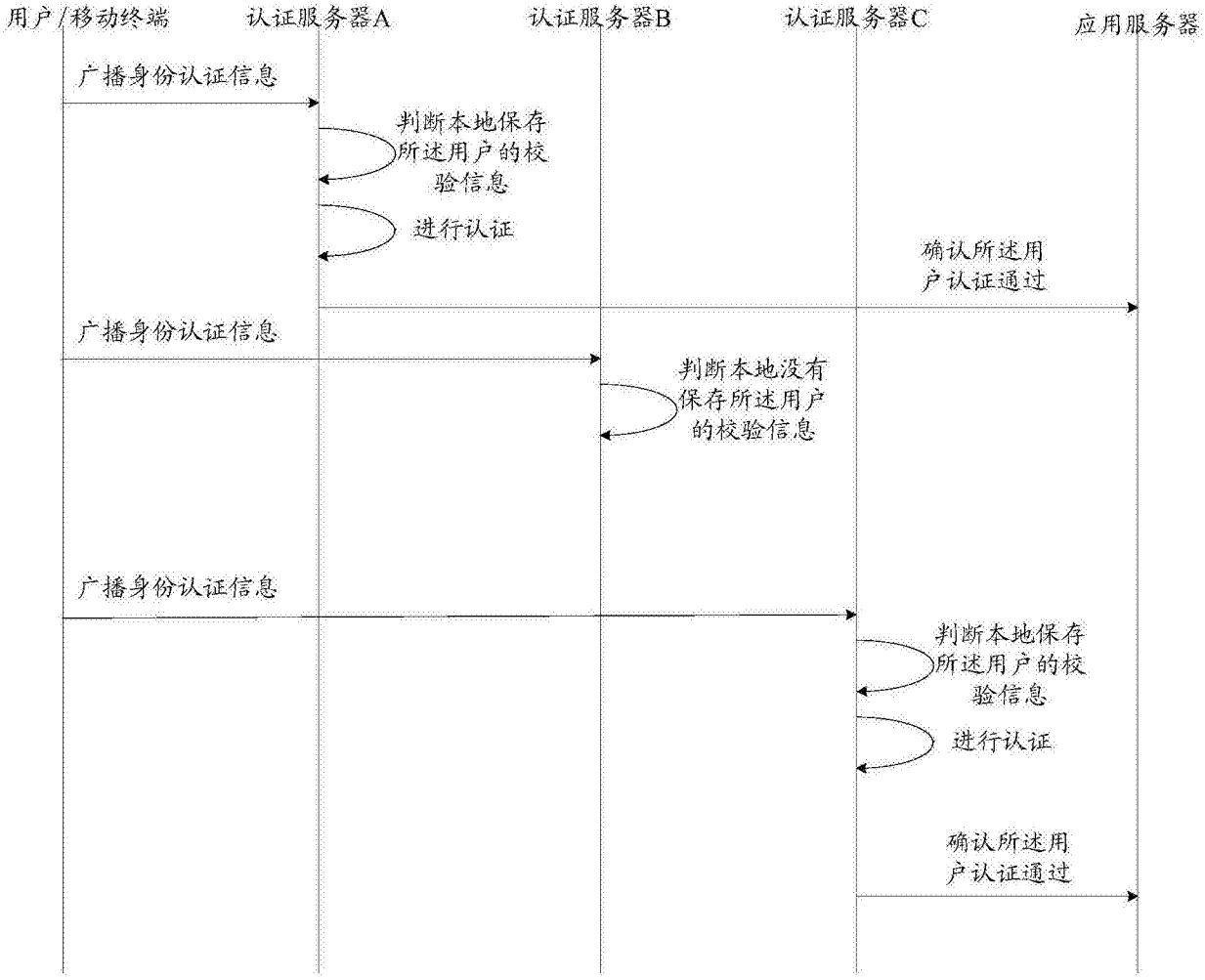

用户/移动终端
认证服务器A
认证服务器B
认证服务器C
应用服务器
广播身份认证信息
判断本地保存
所述用户的校
验信息
进行认证
确认所述用
户认证通过
广播身份认证信息
判断本地没有
保存所述用户
的校验信息
广播身份认证信息
判断本地保存
所述用户的校
验信息
进行认证
确认所述用
户认证通过

图2

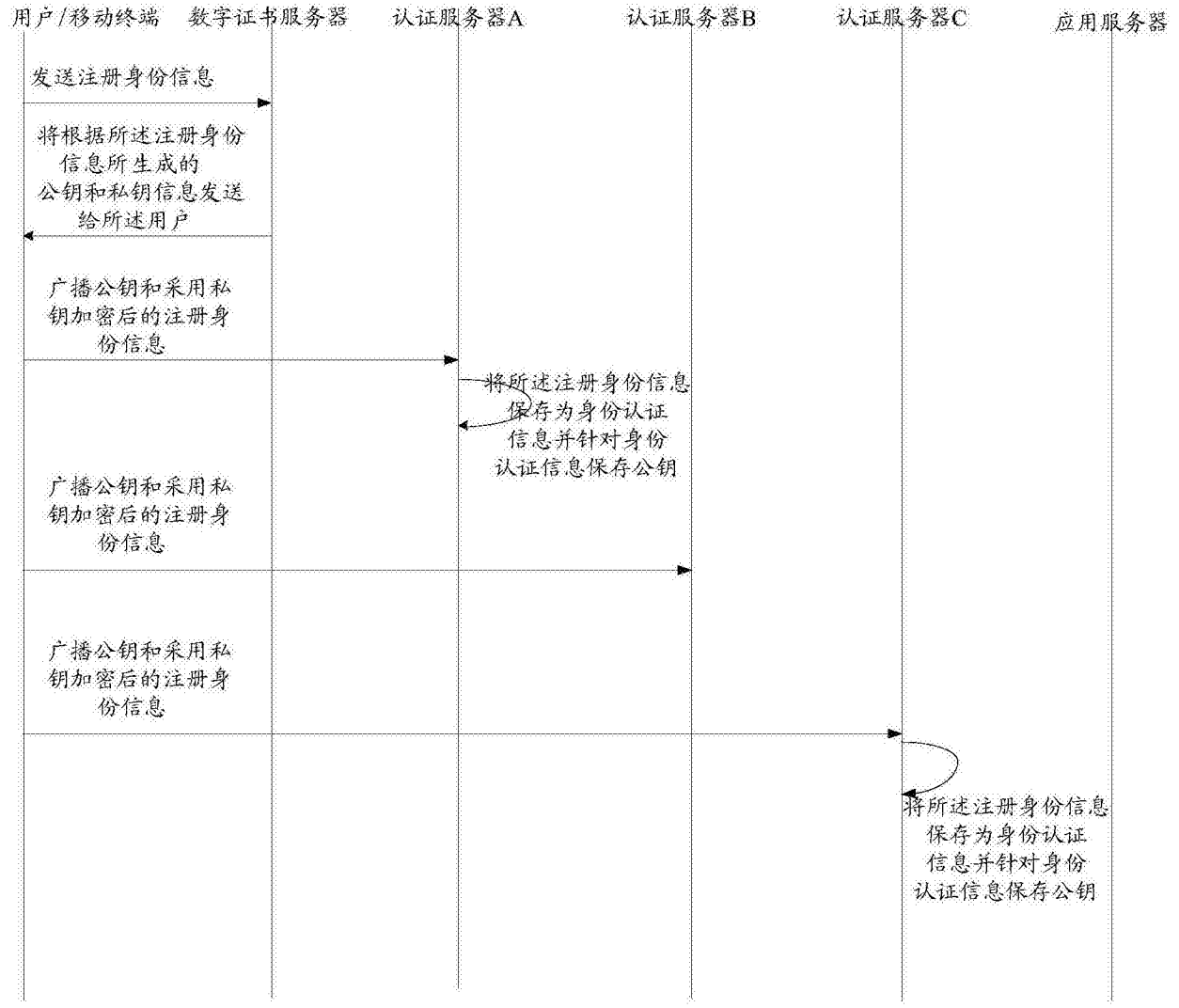

用户/移动终端
数字证书服务器
认证服务器A
认证服务器B
认证服务器C
应用服务器
发送注册身份信息
将根据所述注册身份信息所生成的公钥和私钥信息发送给所述用户
广播公钥和采用私钥加密后的注册身份信息
将所述注册身份信息保存为身份认证信息并针对身份认证信息保存公钥
广播公钥和采用私钥加密后的注册身份信息
广播公钥和采用私钥加密后的注册身份信息
将所述注册身份信息保存为身份认证信息并针对身份认证信息保存公钥

图3

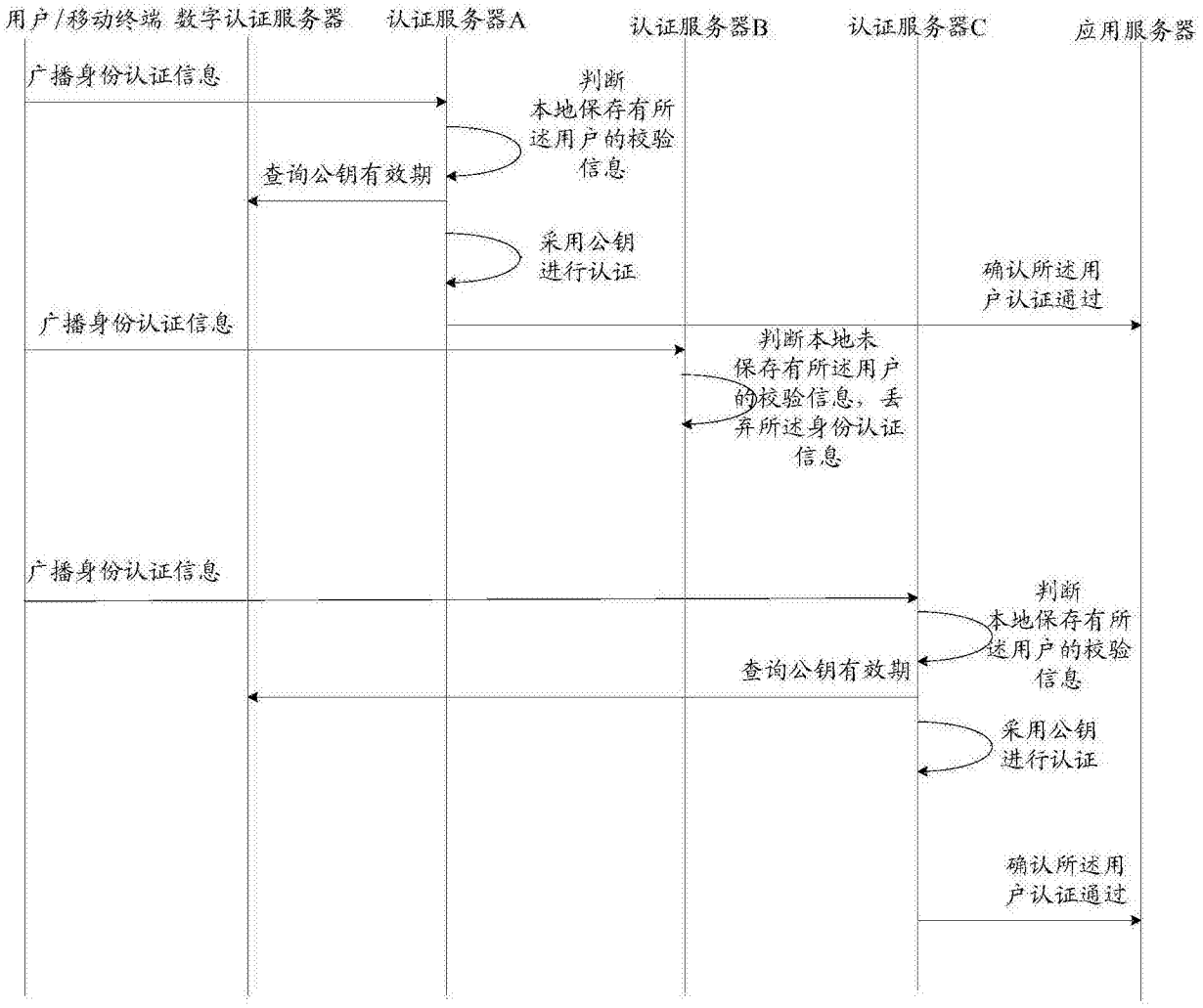

用户/移动终端
数字认证服务器
认证服务器A
认证服务器B
认证服务器C
应用服务器
广播身份认证信息
判断本地保存有所述用户的校验信息
查询公钥有效期
采用公钥进行认证
确认所述用户认证通过
广播身份认证信息
判断本地未保存有所述用户的校验信息，丢弃所述身份认证信息
广播身份认证信息
判断本地保存有所述用户的校验信息
查询公钥有效期
采用公钥进行认证
确认所述用户认证通过

图4

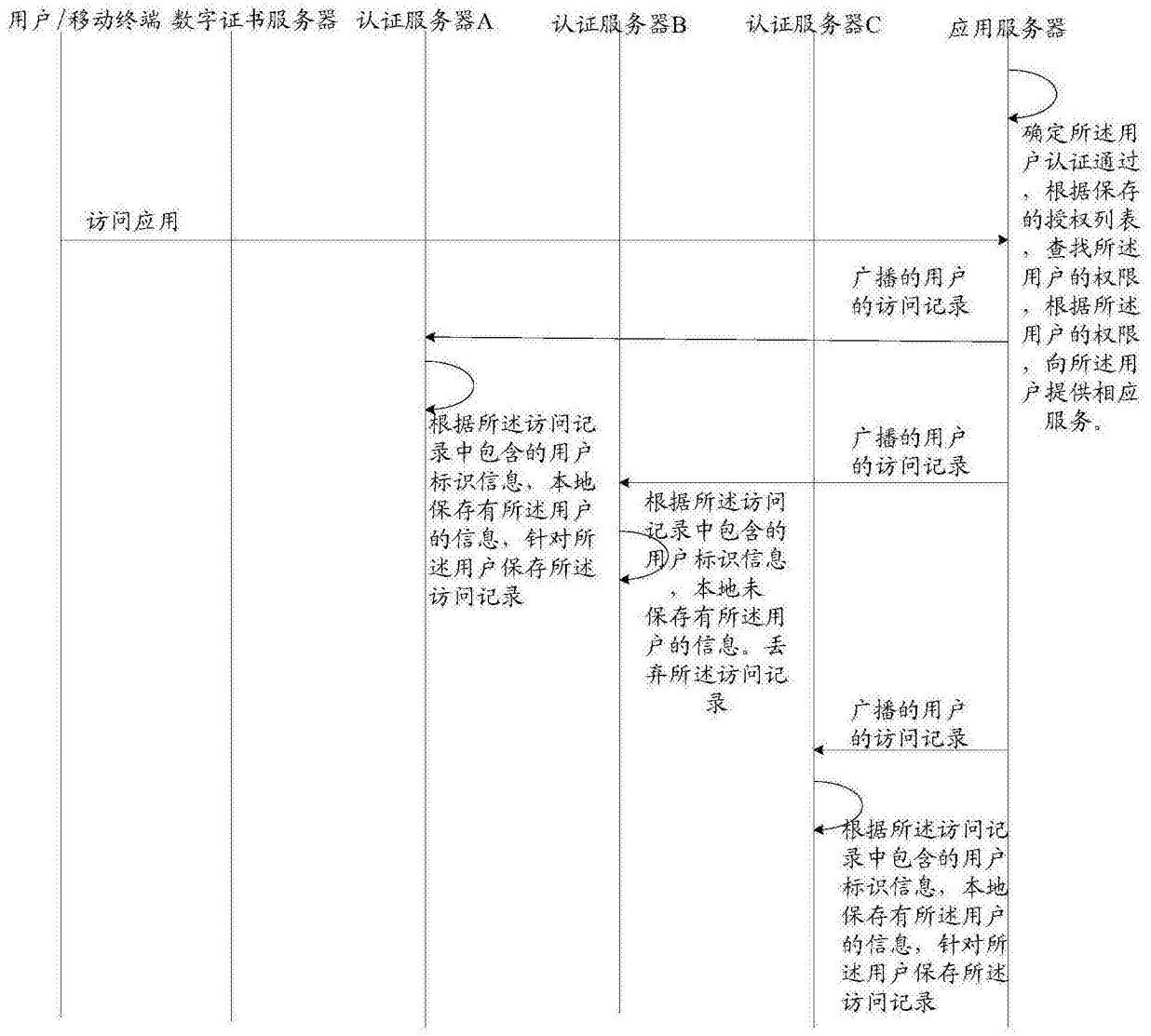

用户/移动终端
数字证书服务器
认证服务器A
认证服务器B
认证服务器C
应用服务器
确定所述用户认证通过，根据保存的授权列表，查找所述用户的权限，根据所述用户的权限，向所述用户提供相应服务。
访问应用
广播的用户的访问记录
根据所述访问记录中包含的用户标识信息，本地保存有所述用户的信息，针对所述用户保存所述访问记录
广播的用户的访问记录
根据所述访问记录中包含的用户标识信息，本地未保存有所述用户的信息。丢弃所述访问记录
广播的用户的访问记录
根据所述访问记录中包含的用户标识信息，本地保存有所述用户的信息，针对所述用户保存所述访问记录

图5

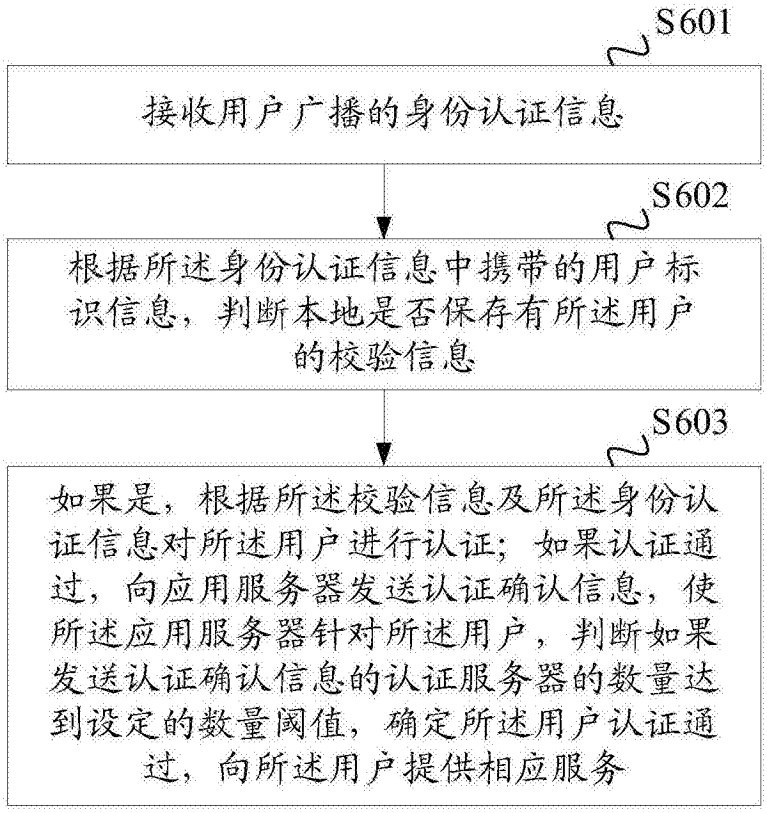

S601
接收用户广播的身份认证信息
S602
根据所述身份认证信息中携带的用户标识信息，判断本地是否保存有所述用户的校验信息
S603
如果是，根据所述校验信息及所述身份认证信息对所述用户进行认证；如果认证通过，向应用服务器发送认证确认信息，使所述应用服务器针对所述用户，判断如果发送认证确认信息的认证服务器的数量达到设定的数量阈值，确定所述用户认证通过，向所述用户提供相应服务

图6

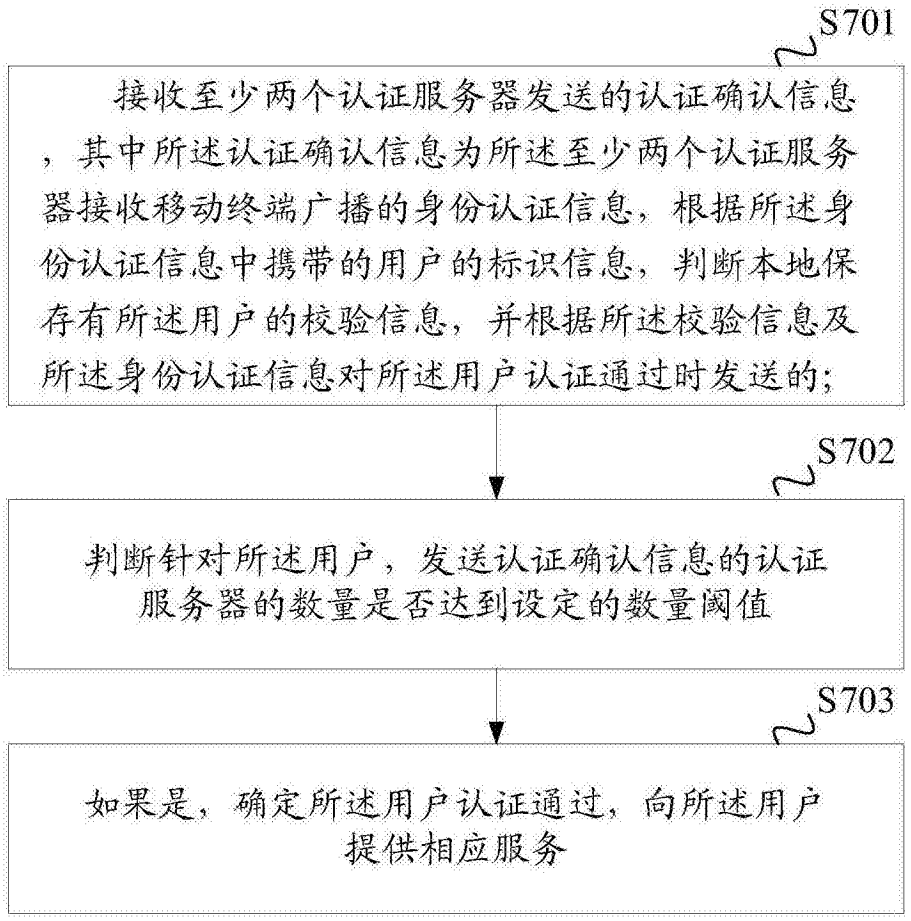

S701
接收至少两个认证服务器发送的认证确认信息，其中所述认证确认信息为所述至少两个认证服务器接收移动终端广播的身份认证信息，根据所述身份认证信息中携带的用户的标识信息，判断本地保存有所述用户的校验信息，并根据所述校验信息及所述身份认证信息对所述用户认证通过时发送的；
S702
判断针对所述用户，发送认证确认信息的认证服务器的数量是否达到设定的数量阈值
S703
如果是，确定所述用户认证通过，向所述用户提供相应服务

图7

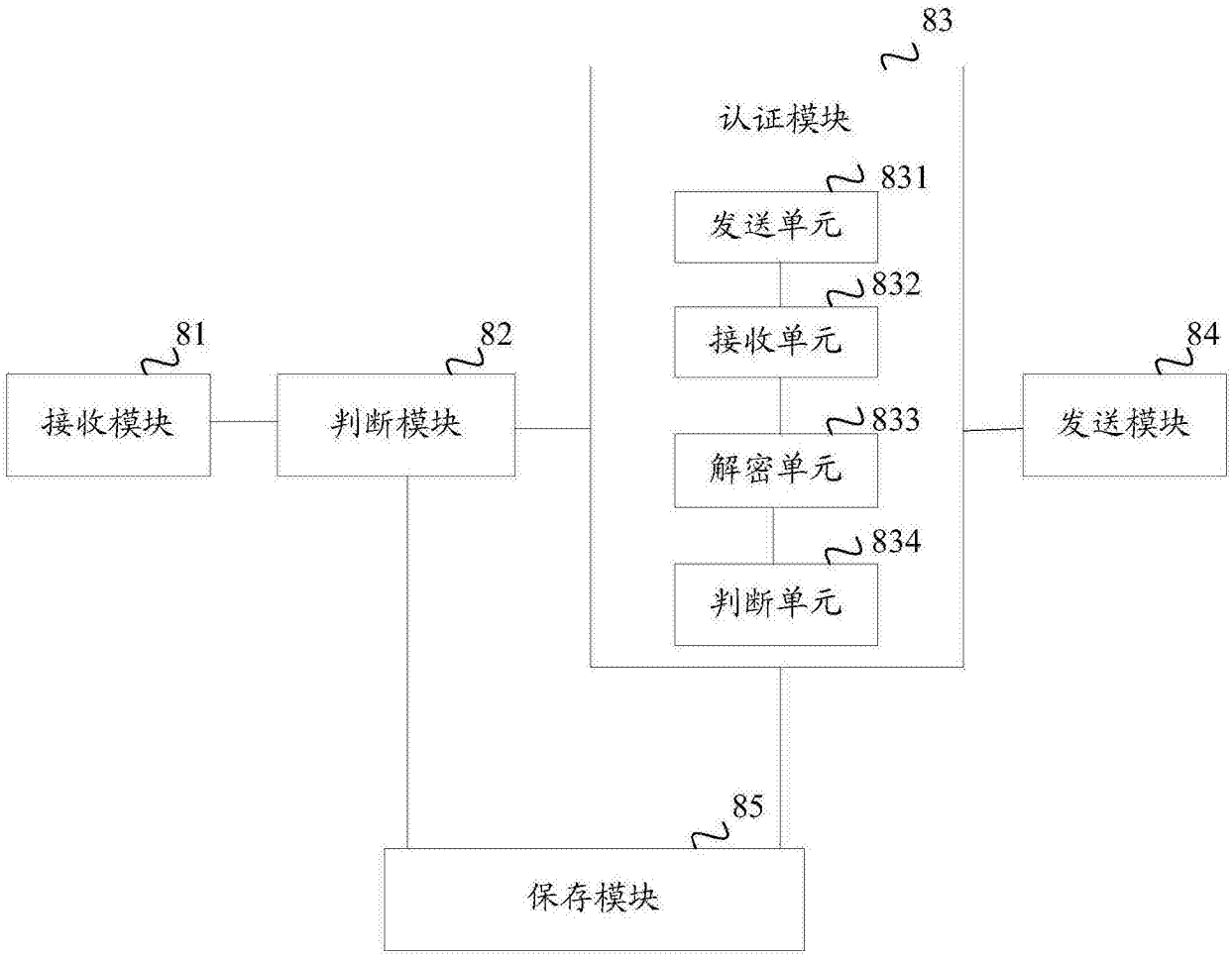

83
认证模块
831
发送单元
832
接收单元
833
解密单元
834
判断单元
81
接收模块
82
判断模块
84
发送模块
85
保存模块

图8

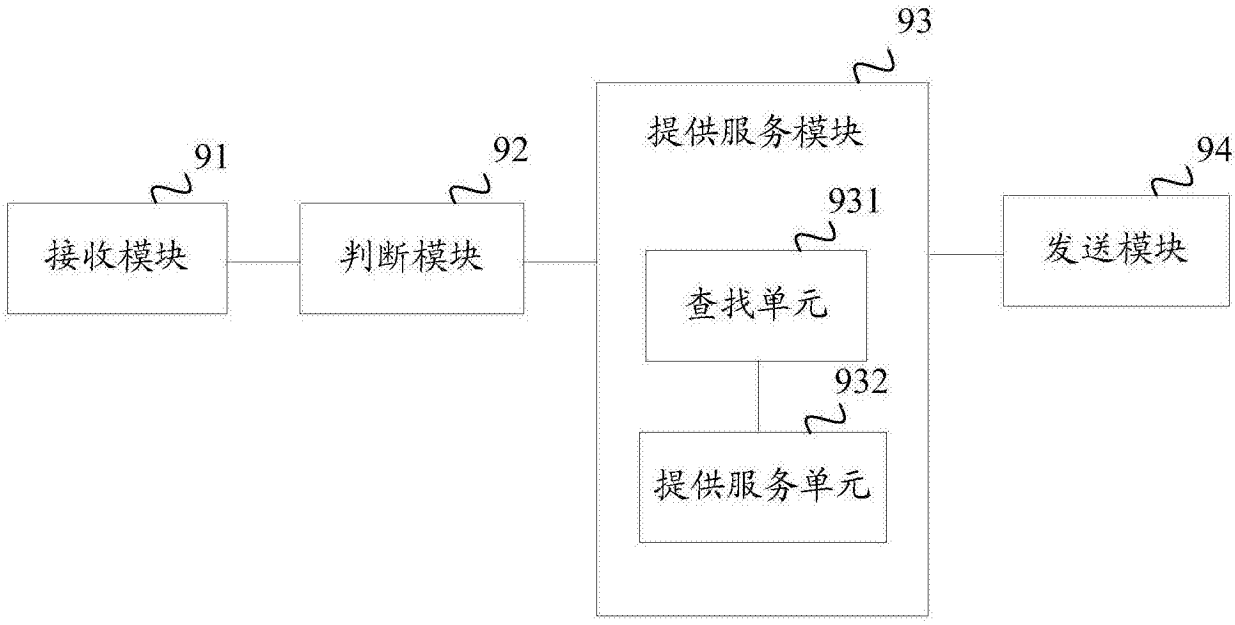

93
提供服务模块
91
接收模块
92
判断模块
931
查找单元
932
提供服务单元
94
发送模块

图9