(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 104023012 A
(43)申请公布日 2014.09.03

(21)申请号 201410239488.3

(22)申请日 2014.05.30

(71)申请人 北京金山网络科技有限公司
地址 100041 北京市石景山区八大处高科技园区西井路 3 号 3 号楼 1592A 房间

(72)发明人 徐友春 马健

(74)专利代理机构 北京清亦华知识产权代理事务所（普通合伙） 11201
代理人 张大威

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

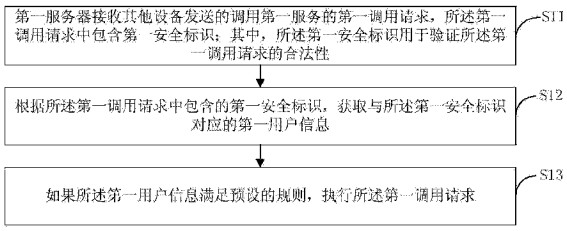
权利要求书3页 说明书9页 附图5页

(54)发明名称

集群中调用服务的方法、设备和系统

(57)摘要

本发明提出一种集群中调用服务的方法、设备和系统，该方法包括第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；第一服务器根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息；如果所述第一用户信息满足预设的规则，第一服务器执行所述第一调用请求。该方法能够实现集群中权限的分发和验证。



CN 104023012 A

1. 一种集群中调用服务的方法，其特征在于，包括：

第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；

第一服务器根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息；

如果所述第一用户信息满足预设的规则，第一服务器执行所述第一调用请求。

2. 根据权利要求 1 所述的方法，其特征在于，所述根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息，包括：

将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证；

如果所述其他设备通过验证，接收所述安全服务器发送的验证信息，所述验证信息中包括所述第一用户信息。

3. 根据权利要求 1 所述的方法，其特征在于，所述根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息，包括：

根据第一安全标识，在第一服务器本地保存的验证信息中进行查找；其中，所述本地保存的验证信息包括：安全标识、用户信息以及对应的过期时间；

若查找到，根据过期时间判断第一安全标识对应的验证信息是否过期；

若所述验证信息未过期，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息。

4. 根据权利要求 1-3 任一项所述的方法，其特征在于，在第一服务器接收其他设备发送的调用第一服务的第一调用请求之前，还包括：

所述其他设备从安全服务器获取第一安全标识。

5. 根据权利要求 4 所述的方法，其特征在于，如果所述其他设备是调用所述第一服务的第二服务器，所述其他设备从安全服务器获取第一安全标识，包括：

所述第二服务器将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器；

安全服务器根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识；

第二服务器接收安全服务器发送的第一安全标识。

6. 根据权利要求 5 所述的方法，其特征在于，安全服务器根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识，包括：

安全服务器分别对接收的第二安全标识以及第二服务器的安全标识进行解密，得到第二安全标识对应的第二 IP 地址和第二用户信息，以及，第二服务器的安全标识对应的第三 IP 地址和第三用户信息；

安全服务器对所述第二 IP 地址、第二用户信息和第三用户信息进行加密，生成所述第一安全标识。

7. 根据权利要求 4 所述的方法，其特征在于，如果所述其他设备是终端设备，所述其他设备从安全服务器获取第一安全标识，包括：

所述终端设备向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的 IP 地址、所述终端设备的用户标识和安全密码；

安全服务器根据所述终端设备的用户标识和安全密码对所述终端设备进行验证；

在验证通过后，安全服务器根据终端设备的用户标识获取终端设备的用户信息，并根据终端设备的 IP 地址以及终端设备的用户信息，采用预设的加密算法得到所述第一安全标识；

所述终端设备接收安全服务器发送的所述第一安全标识。

8. 第一服务器，其特征在于，包括：

接收模块，用于接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；

获取模块，用于根据第一安全标识，获取与所述第一安全标识对应的第一用户信息；

处理模块，用于在所述第一用户信息满足预设的规则时，执行所述第一调用请求。

9. 根据权利要求 8 所述的第一服务器，其特征在于，所述获取模块包括：

发送子模块，用于将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证；

接收子模块，如果所述其他设备通过验证，用于接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标识对应的第一用户信息。

10. 根据权利要求 9 所述的第一服务器，其特征在于，所述获取模块还包括：

保存子模块，用于将所述验证信息保存在本地。

11. 根据权利要求 8 所述的第一服务器，其特征在于，所述获取模块包括：

查找子模块，用于根据第一安全标识，在所述第一服务器本地保存的验证信息中进行查找；若查找到，触发验证子模块；

验证子模块，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息。

12. 一种通信系统，其特征在于，包括：如权利要求 8-11 任一项所述的第一服务器、终端设备以及安全服务器，其中：

所述终端设备，用于向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的 IP 地址、所述终端设备的用户标识和安全密码；接收安全服务器发送的第一安全标识；

所述安全服务器，用于根据该终端设备的用户标识和安全密码对终端设备进行验证，在验证通过后，根据终端设备的用户标识获取终端设备的用户信息，并根据终端设备的 IP 地址以及终端设备的用户信息，采用预设的加密算法得到第一安全标识。

13. 一种通信系统，其特征在于，包括：如权利要求 8-11 任一项所述的第一服务器、第二服务器以及安全服务器，其中：

所述第二服务器，用于将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器，接收安全服务器发送的第一安全标识；

所述安全服务器，用于根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识。

14. 根据权利要求 13 所述的通信系统，其特征在于，所述安全服务器，具体用于分别对接收的第二安全标识以及第二服务器的安全标识进行解密，得到第二安全标识对应的第二 IP 地址和第二用户信息，以及，第二服务器的安全标识对应的第三 IP 地址和第三用户信

息，安全服务器可以对第二 IP 地址、第二用户信息和第三用户信息进行加密，生成上述第一安全标识。

集群中调用服务的方法、设备和系统

技术领域

[0001] 本发明涉及集群安全技术领域，尤其涉及一种集群中调用服务的方法、设备和系统。

背景技术

[0002] 集群中会包含多个服务，一个服务可以被其他服务或客户端调用，为了保证集群的安全性，需要调用服务的调用者具有相应的权限。

[0003] 集群中可能会涉及多层验证，例如，在客户端调用一个服务时，该服务在执行时可能会再调用另一个服务。因此，需要解决集群中的权限分发及验证的问题。

发明内容

[0004] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0005] 为此，本发明的一个目的在于提出一种集群中调用服务的方法，该方法可以实现集群中的权限分发及验证。

[0006] 本发明的另一个目的在于提出一种服务器。

[0007] 本发明的另一个目的在于提出一种通信系统。

[0008] 为达到上述目的，本发明第一方面实施例提出的集群中调用服务的方法，包括：第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；第一服务器根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息；如果所述第一用户信息满足预设的规则，第一服务器执行所述第一调用请求。

[0009] 本发明第一方面实施例提出的集群中调用服务的方法，第一服务器采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0010] 为达到上述目的，本发明第二方面实施例提出的第一服务器，包括：接收模块，用于接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；获取模块，用于根据第一安全标识，获取与所述第一安全标识对应的第一用户信息；处理模块，用于在所述第一用户信息满足预设的规则时，执行所述第一调用请求。

[0011] 本发明第二方面实施例提出的第一服务器，采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0012] 为达到上述目的，本发明第三方面实施例提出的通信系统，包括：第二方面实施例提出的第一服务器、终端设备以及安全服务器，其中：所述终端设备，用于向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的 IP 地址、所述终端设备的用户标识和安全密码；接收安全服务器发送的第一安全标识；所述安全服务器，用于

根据该终端设备的用户标识和安全密码对终端设备进行验证，在验证通过后，根据终端设备的用户标识获取终端设备的用户信息，并根据终端设备的 IP 地址以及终端设备的用户信息，采用预设的加密算法得到第一安全标识。

[0013] 本发明第三方面实施例提出的通信系统，第一服务器采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0014] 为达到上述目的，本发明第四方面实施例提出的通信系统，包括：如本发明第二方面实施例所述的第一服务器、第二服务器以及安全服务器，其中：所述第二服务器，用于将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器，接收安全服务器发送的第一安全标识；所述安全服务器，用于根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识。

[0015] 本发明第四方面实施例提出的通信系统，第一服务器采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0016] 为达到上述目的，本发明第五方面实施例提出的服务器，包括：壳体、处理器、存储器、电路板和电源电路，其中，电路板安置在壳体围成的空间内部，处理器和存储器设置在电路板上；电源电路，用于为该系统的各个电路或器件供电；存储器用于存储可执行程序代码；处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序，以用于执行：接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性；根据所述第一安全标识，获取与所述第一安全标识对应的第一用户信息；如果所述第一用户信息满足预设的规则，第一服务器执行所述第一调用请求。

[0017] 本发明第五方面实施例提出的服务器，采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0018] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0019] 本发明上述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0020] 图 1 是本发明一实施例提出的集群中调用服务的方法的流程示意图；

[0021] 图 2 是本发明实施例中 S12 的一种具体实现流程示意图；

[0022] 图 3a 是本发明实施例中 S12 的另一种具体实现流程示意图；

[0023] 图 3b 是本发明实施例中 S12 的另一种具体实现流程示意图；

[0024] 图 4 是本发明另一实施例提出的集群中调用服务的方法的流程示意图；

[0025] 图 5 是本发明实施例中 S10 的一种具体实现流程示意图；

[0026] 图 6 是本发明实施例中 S10 的另一种具体实现流程示意图；

[0027] 图 7 是本发明一实施例提出的第一服务器的结构示意图；

[0028] 图 8a 是本发明另一实施例提出的第一服务器的结构示意图；

[0029] 图 8b 是本发明另一实施例提出的第一服务器的结构示意图；

[0030] 图 8c 是本发明另一实施例提出的第一服务器的结构示意图；

[0031] 图 9 是本发明一实施例提出的通信系统的结构示意图；

[0032] 图 10 是本发明另一实施例提出的通信系统的结构示意图。

具体实施方式

[0033] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0034] 图 1 是本发明一实施例提出的集群中调用服务的方法的流程示意图，该方法包括：

[0035] S11：第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性。

[0036] 其中，第一服务器可以是集群系统中的某一个服务器，在第一服务器上运行至少一个服务，其中包括将第一服务。

[0037] 其他设备可以为终端设备，例如，手机、个人电脑 (Personal Computer，PC) 或平板电脑等。或者，其他设备可以为集群中的某个服务器，例如，运行第二服务的服务器等。

[0038] 具体的，当其他设备是终端设备时，该第一安全标识是终端设备的安全标识。

[0039] 当其他设备是集群中的服务器时，假设为第二服务器，该第一安全标识，是根据第二服务器的安全标识以及发送给第二服务器的第二调用请求中包含的第二安全标识生成的标识。

[0040] 可选的，在本发明的一个具体实现中，可以根据设备的 IP 地址以及设备的用户信息，预先由安全服务器采用预设的加密算法得到安全标识；其中，加密处理的算法可以为数据加密标准 (Data Encryption Standard，DES) 算法或者高级加密标准 (Advanced Encryption Standard，AES) 算法。

[0041] 安全服务器是集群系统中的一个服务器，其上运行了安全服务，安全服务用于为终端设备或者集群中运行的其他服务分发安全标识，并对来自其他服务的安全标识进行验证。

[0042] 设备的用户信息可以包括：设备的权限信息和 / 或设备的用户标识。例如，权限信息可以是管理员权限和普通用户，普通用户可以包括游客、一级用户、二级用户等；用户标识可以为设备的用户名。

[0043] S12：根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息。

[0044] S13：如果所述第一用户信息满足预设的规则，执行所述第一调用请求。

[0045] 可选的，上述预设的规则可以是：管理员能够调用第一服务。对应的，当第一用户

信息包括的权限信息为管理员权限时，就可以执行该第一调用请求。或者，上述预设的规则可以是：指定的用户 ID 组能够调用第一服务。那么当第一用户信息中包括的用户标识属于该用户 ID 组时，就可以执行该第一调用请求。

[0046] 可选的，在本发明的实施例中，如果第一服务执行第一调用请求，可以向其他设备反馈调用成功的应答。当然，如果所述第一用户信息不满足预设规则，可以拒绝执行所述第一调用请求，向其他设备反馈无权调用应答或调用错误应答。

[0047] 可选的，如图 2 所示，在本发明的一个具体实现中，根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息 (S12)，可以包括：

[0048] S121：第一服务器将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证；

[0049] S122：如果所述其他设备通过验证，第一服务器接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标记对应的第一用户信息。

[0050] 可选的，如图 3a 所示，在本发明的另一个具体实现中，在上述 S122 之后，上述 S12 还可以包括：

[0051] S123：第一服务器将所述验证信息保存在本地。

[0052] 可选的，上述验证信息中还可以包括安全标识和过期时间，第一服务器可以将安全标识、用户信息和过期时间对应保存。

[0053] 示例性的，安全服务器可以采用如下方式对其他设备进行安全验证：

[0054] 采用预设的解密算法对第一安全标识进行解密，如果解密成功，从解密后的信息中获取第一 IP 地址和第一用户信息；根据安全服务器上预先保存的与该第一安全标识对应的设备 IP 地址与设备用户信息，确定解密得到的第一 IP 地址和第一用户信息是否准确，如果准确，则所述其他设备通过验证，否则，所述其他设备未通过验证。例如，如果解密不成功或者解密得到的第一 IP 地址与第一用户信息和第一安全标识的对应关系不准确，则所述其他设备未通过验证。

[0055] 可选的，如图 3b 所示，在本发明的又一个具体实现中，根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息 (S12)，可以包括：

[0056] S124：根据第一安全标识，在第一服务器本地保存的验证信息中进行查找；

[0057] S125：若查找到，根据过期时间判断第一安全标识对应的验证信息是否过期；

[0058] S126：若所述验证信息未过期，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息。

[0059] 可选的，如图 4 所示，在本发明另一实施例中，上述 S11 之前，集群中调用服务的方法还可以包括：

[0060] S10：其他设备从安全服务器获取第一安全标识。

[0061] 示例性的，当其他设备是调用第一服务的第二服务器时，如图 5 所示，上述 S10 可以包括：

[0062] S51：第二服务器将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器。

[0063] S52：安全服务器根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识。

[0064] 其中，安全服务器可以分别对接收的两个安全标识进行解密，得到第二安全标识对应的第二 IP 地址和第二用户信息，以及，第二服务器的安全标识对应的第三 IP 地址和第三用户信息，安全服务器可以对第二 IP 地址、第二用户信息和第三用户信息进行加密，生成上述第一安全标识。

[0065] S53 ：第二服务器接收安全服务器发送的第一安全标识。

[0066] 示例性的，参见图 6，当其他设备是终端设备时，上述 S10 可以包括

[0067] S61 ：终端设备向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的 IP 地址、所述终端设备的用户标识和安全密码。

[0068] S62 ：安全服务器根据该终端设备的用户标识和安全密码对终端设备进行验证。

[0069] S63 ：在验证通过后，安全服务器根据终端设备的用户标识获取终端设备的用户信息，例如，用户权限，并根据终端设备的 IP 地址以及终端设备的用户信息，采用预设的加密算法得到上述第一安全标识 ；其中，终端设备的用户信息包括终端设备的用户标识和 / 或终端设备的用户权限。

[0070] 在本发明的实施例中，安全服务器中还可以预先配置每个设备的用户标识对应的用户权限，因此，安全服务器可以根据预先的配置，获取其他设备的用户标识对应的用户权限。

[0071] 用户权限可以用字符串标识，例如，当权限分为管理员权限和普通用户权限时，管理员权限可以用 1 表示，普通用户权限可以用 2 表示。

[0072] S64 ：终端设备接收安全服务器发送的第一安全标识。

[0073] 在本发明的实施例中，第一服务器、第二服务器、安全服务器等，均为从功能角度的命名，可能部署在同一实体设备上 ；也可能部署在不同的实体设备上。本发明的实施例对此不做具体限定。

[0074] 本实施例中，第一服务器采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0075] 图 7 是本发明一实施例提出的第一服务器的结构示意图，该第一服务器包括接收模块 71、获取模块 72 和处理模块 73。

[0076] 接收模块 71 用于接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识 ；其中，所述第一安全标识所述第一安全标识用于验证所述第一调用请求的合法性 ；

[0077] 获取模块 72 用于根据第一安全标识，获取与所述第一安全标识对应的第一用户信息 ；

[0078] 处理模块 73 用于在所述第一用户信息满足预设的规则时，执行所述第一调用请求。

[0079] 可选的，在本发明的一个实施例中，如图 8a 所示，所述获取模块 72 可以包括 ：

[0080] 发送子模块 721，用于将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证 ；

[0081] 接收子模块 722，如果所述其他设备通过验证，用于接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标识对应的第一用户信息。

[0082] 进一步的，如图 8b 所示，所述获取模块 72 还可以包括 ：

[0083] 保存子模块 723，用于将所述验证信息保存在本地。

[0084] 可选的，在本发明的又一个实施例中，如图 8c 所示，所述获取模块 72 还可以包括 ：

[0085] 查找子模块 724，用于根据第一安全标识，在所述第一服务器本地保存的验证信息中进行查找 ；若查找到，触发验证子模块 725 ；

[0086] 验证子模块 725，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息。

[0087] 该第一服务器的具体功能可以参见上述方法中对第一服务器的描述，在此不再赘述。

[0088] 本实施例中，通过采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0089] 本发明实施例还提出了一种通信系统，如图 9 所示，包括第一服务器 91，终端设备 92 以及安全服务器 93，其中 ：

[0090] 第一服务器 91 可以是如图 7- 图 8c 中任一所示的设备。

[0091] 终端设备 92 用于向安全服务器 93 发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备 92 的 IP 地址、所述终端设备 92 的用户标识和安全密码 ；接收安全服务器 93 发送的第一安全标识。

[0092] 安全服务器 93 用于根据该终端设备 92 的用户标识和安全密码对终端设备 92 进行验证，在验证通过后，根据终端设备 92 的用户标识获取终端设备 92 的用户信息，例如，用户权限，并根据终端设备 92 的 IP 地址以及终端设备 92 的用户信息，采用预设的加密算法得到第一安全标识。

[0093] 本发明实施例还提出了另一种通信系统，如图 10 所示，包括第一服务器 101，第二服务器 102 以及安全服务器 103，其中 ：

[0094] 第一服务器 101 可以是如图 7- 图 8c 中任一所示的设备。

[0095] 第二服务器 102 用于将接收到的第二调用请求中包含的第二安全标识和第二服务器 102 的安全标识发送给安全服务器 103，接收安全服务器 103 发送的第一安全标识。

[0096] 安全服务器 103 用于根据接收的第二安全标识以及第二服务器 102 的安全标识，生成上述第一安全标识。

[0097] 例如，安全服务器 103 可以分别对接收的两个安全标识进行解密，得到第二安全标识对应的第二 IP 地址和第二用户信息，以及，第二服务器 102 的安全标识对应的第三 IP 地址和第三用户信息，安全服务器 103 可以对第二 IP 地址、第二用户信息和第三用户信息进行加密，生成上述第一安全标识。

[0098] 本发明实施例还提供了一种第一服务器，该第一服务器包括壳体、处理器、存储器、电路板和电源电路，其中，电路板安置在壳体围成的空间内部，处理器和存储器设置在电路板上 ；电源电路，用于为第一服务器的各个电路或器件供电 ；存储器用于存储可执行程序代码 ；处理器通过读取存储器中存储的可执行程序代码来运行与可执行程序代码对应的程序，以用于执行 ：

[0099] S11’：接收其他设备发送的调用第一服务的第一调用请求，所述调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性。

[0100] 其中，第一服务器可以是集群系统中的某一个服务器，在第一服务器上运行至少一个服务，其中包括将第一服务。

[0101] 其他设备可以为终端设备，例如，手机、个人电脑 (Personal Computer，PC) 或平板电脑等。或者，其他设备可以为集群中的某个服务器，例如，运行第二服务的服务器等。

[0102] 具体的，当其他设备是终端设备时，该第一安全标识是终端设备的安全标识。

[0103] 当其他设备是集群中的服务器时，假设为第二服务器，该第一安全标识，是根据第二服务器的安全标识以及发送给第二服务器的第二调用请求中包含的第二安全标识生成的标识。

[0104] 可选的，在本发明的一个具体实现中，可以根据设备的 IP 地址以及设备的用户信息，预先由安全服务器采用预设的加密算法得到安全标识；其中，加密处理的算法可以为数据加密标准 (Data Encryption Standard，DES) 算法或者高级加密标准 (Advanced Encryption Standard，AES) 算法。

[0105] 安全服务器是集群系统中的一个服务器，其上运行了安全服务，安全服务用于为终端设备或者集群中运行的其他服务分发安全标识，并对来自其他服务的安全标识进行验证。

[0106] 设备的用户信息可以包括：设备的权限信息和 / 或设备的用户标识。例如，权限信息可以是管理员权限和普通用户，普通用户可以包括游客、一级用户、二级用户等；用户标识可以为设备的用户名。

[0107] S12’：根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息。

[0108] S13’：如果所述第一用户信息满足预设的规则，执行所述第一调用请求。

[0109] 可选的，上述预设的规则可以是：管理员能够调用第一服务。对应的，当第一用户信息包括的权限信息为管理员权限时，就可以执行该第一调用请求。或者，上述预设的规则可以是：指定的用户 ID 组能够调用第一服务。那么当第一用户信息中包括的用户标识属于该用户 ID 组时，就可以执行该第一调用请求。

[0110] 可选的，在本发明的实施例中，如果第一服务执行第一调用请求，可以向其他设备反馈调用成功的应答。当然，如果所述第一用户信息不满足预设规则，可以拒绝执行所述第一调用请求，向其他设备反馈无权调用应答或调用错误应答。

[0111] 可选的，在本发明的一个具体实现中，根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息 (S12)，可以包括：

[0112] S121’：第一服务器将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证；

[0113] S122’：如果所述其他设备通过验证，第一服务器接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标记对应的第一用户信息。

[0114] 可选的，在本发明的另一个具体实现中，在上述 S122 之后，上述 S12 还可以包括：

[0115] S123’：第一服务器将所述验证信息保存在本地。

[0116] 可选的，上述验证信息中还可以包括安全标识和过期时间，第一服务器可以将安

全标识、用户信息和过期时间对应保存。

[0117] 示例性的，安全服务器可以采用如下方式对其他设备进行安全验证：

[0118] 采用预设的解密算法对第一安全标识进行解密，如果解密成功，从解密后的信息中获取第一 IP 地址和第一用户信息；根据安全服务器上预先保存的与该第一安全标识对应的设备 IP 地址与设备用户信息，确定解密得到的第一 IP 地址和第一用户信息是否准确，如果准确，则所述其他设备通过验证，否则，所述其他设备未通过验证。例如，如果解密不成功或者解密得到的第一 IP 地址与第一用户信息和第一安全标识的对应关系不准确，则所述其他设备未通过验证。

[0119] 可选的，在本发明的又一个具体实现中，根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息 (S12)，可以包括：

[0120] S124’：根据第一安全标识，在第一服务器本地保存的验证信息中进行查找；

[0121] S125’：若查找到，根据过期时间判断第一安全标识对应的验证信息是否过期；

[0122] S126’：若所述验证信息未过期，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息。

[0123] 可选的，在本发明另一实施例中，上述 S11’之前，集群中调用服务的方法还可以包括：

[0124] S10’：其他设备从安全服务器获取第一安全标识。

[0125] 示例性的，当其他设备是调用第一服务的第二服务器时，上述 S10’可以包括：

[0126] S51’：第二服务器将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器。

[0127] S52’：安全服务器根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识。

[0128] 其中，安全服务器可以分别对接收的两个安全标识进行解密，得到第二安全标识对应的第二 IP 地址和第二用户信息，以及，第二服务器的安全标识对应的第三 IP 地址和第三用户信息，安全服务器可以对第二 IP 地址、第二用户信息和第三用户信息进行加密，生成上述第一安全标识。

[0129] S53’：第二服务器接收安全服务器发送的第一安全标识。

[0130] 示例性的，当其他设备是终端设备时，上述 S10’可以包括

[0131] S61’：终端设备向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的 IP 地址、所述终端设备的用户标识和安全密码。

[0132] S62’：安全服务器根据该终端设备的用户标识和安全密码对终端设备进行验证。

[0133] S63’：在验证通过后，安全服务器根据终端设备的用户标识获取终端设备的用户信息，例如，用户权限，并根据终端设备的 IP 地址以及终端设备的用户信息，采用预设的加密算法得到上述第一安全标识；其中，终端设备的用户信息包括终端设备的用户标识和 / 或终端设备的用户权限。

[0134] 在本发明的实施例中，安全服务器中还可以预先配置每个设备的用户标识对应的用户权限，因此，安全服务器可以根据预先的配置，获取其他设备的用户标识对应的用户权限。

[0135] 用户权限可以用字符串标识，例如，当权限分为管理员权限和普通用户权限时，管

理员权限可以用 1 表示，普通用户权限可以用 2 表示。

[0136] S64'：终端设备接收安全服务器发送的第一安全标识。

[0137] 在本发明的实施例中，第一服务器、第二服务器、安全服务器等，均为从功能角度的命名，可能部署在同一实体设备上；也可能部署在不同的实体设备上。本发明的实施例对此不做具体限定。

[0138] 本实施例中，第一服务器采用由集群中安全服务分发的安全标识，并在执行调用请求之前根据该安全标识通过安全服务对调用者进行验证，可以实现集群中的权限分发和验证，保证集群的安全性。

[0139] 需要说明的是，在本发明的描述中，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0140] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0141] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列 (PGA)，现场可编程门阵列 (FPGA) 等。

[0142] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0143] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块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时，也可以存储在一个计算机可读取存储介质中。

[0144] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0145] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0146] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

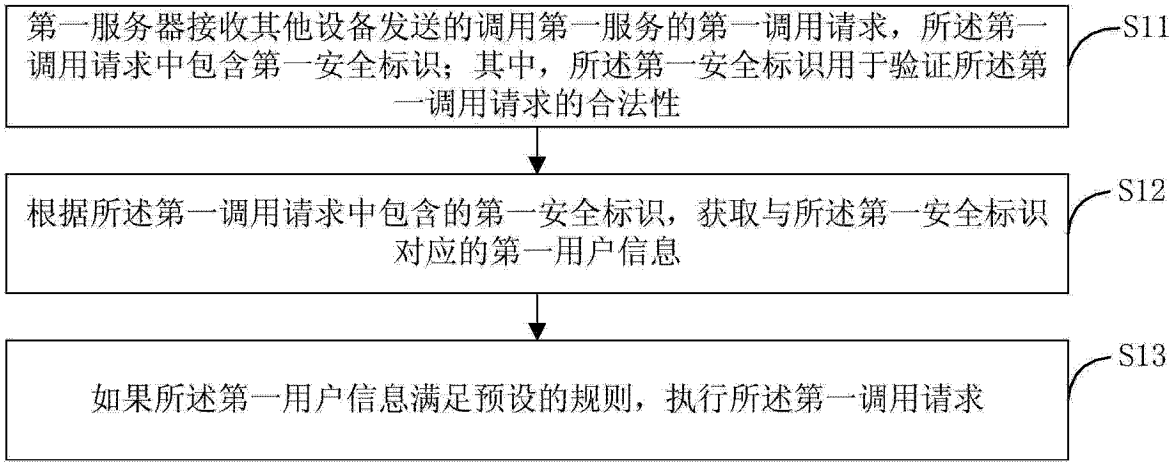

第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性
S11
根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息
S12
如果所述第一用户信息满足预设的规则，执行所述第一调用请求
S13

图 1

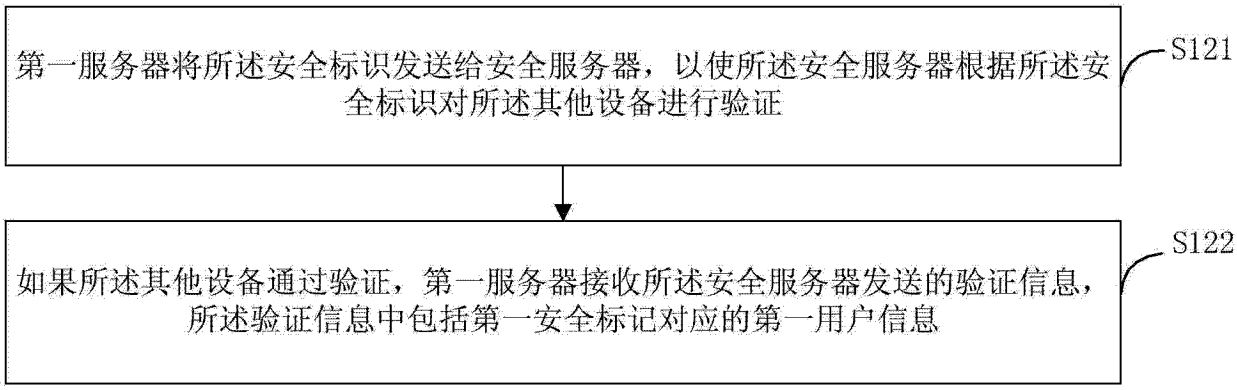

第一服务器将所述安全标识发送给安全服务器，以使所述安全服务器根据所述安全标识对所述其他设备进行验证
S121
如果所述其他设备通过验证，第一服务器接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标记对应的第一用户信息
S122

图 2

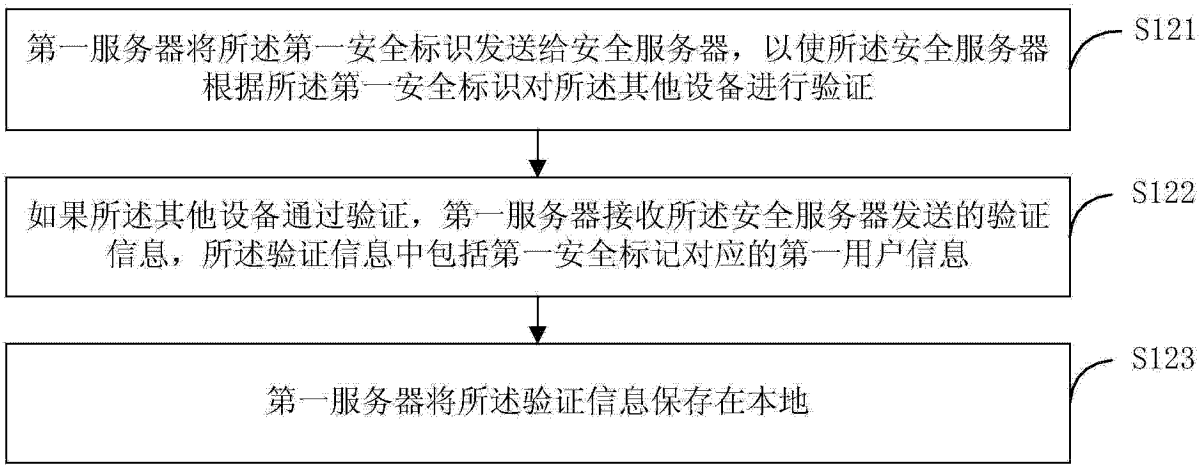

第一服务器将所述第一安全标识发送给安全服务器，以使所述安全服务器根据所述第一安全标识对所述其他设备进行验证
S121
如果所述其他设备通过验证，第一服务器接收所述安全服务器发送的验证信息，所述验证信息中包括第一安全标记对应的第一用户信息
S122
第一服务器将所述验证信息保存在本地
S123

图 3a

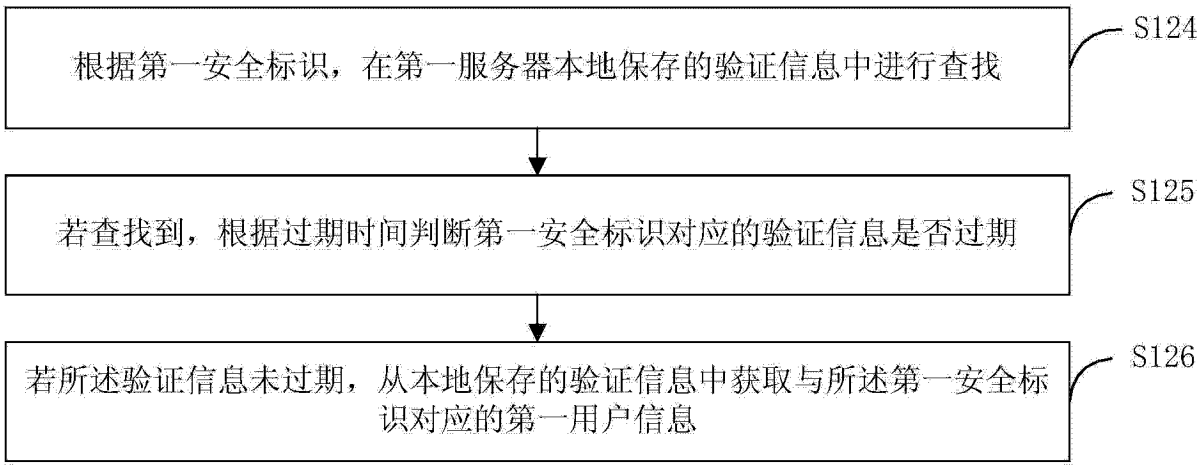

根据第一安全标识，在第一服务器本地保存的验证信息中进行查找
S124
若查找到，根据过期时间判断第一安全标识对应的验证信息是否过期
S125
若所述验证信息未过期，从本地保存的验证信息中获取与所述第一安全标识对应的第一用户信息
S126

图 3b

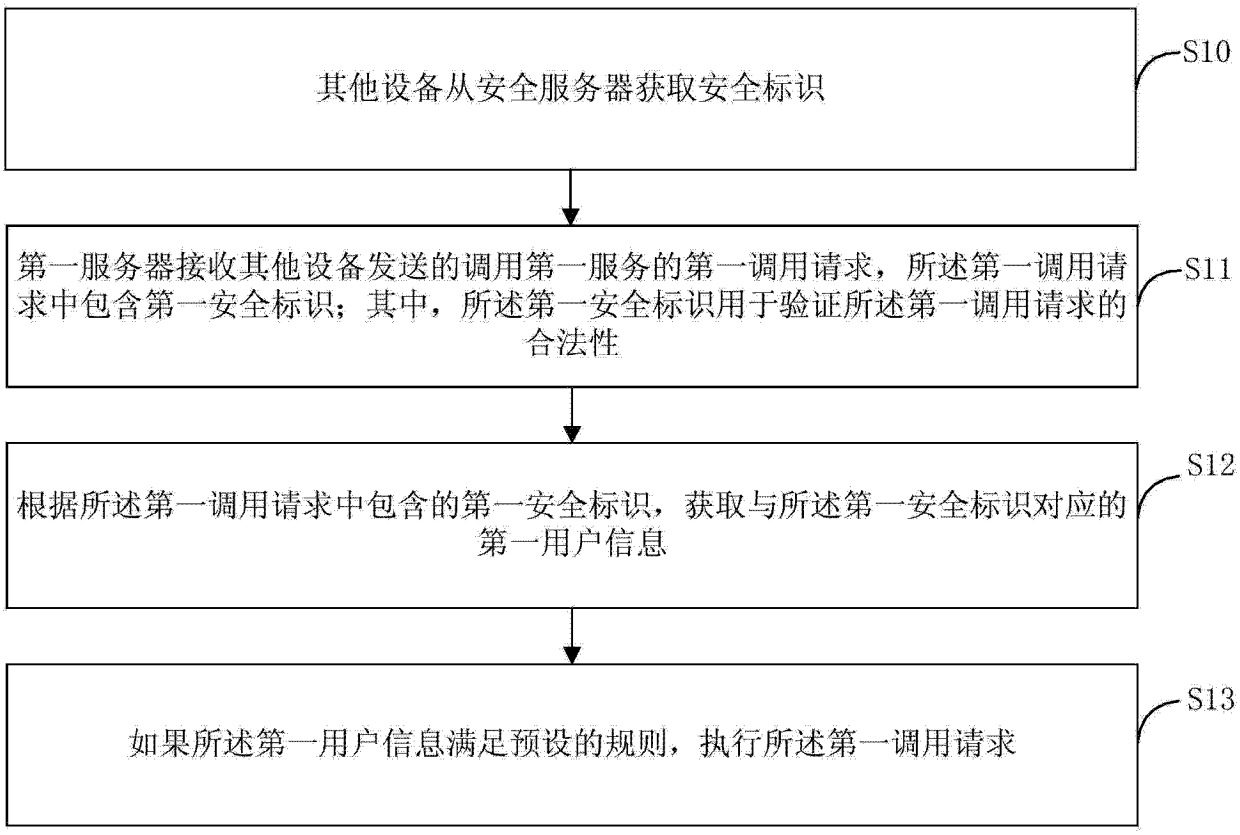

其他设备从安全服务器获取安全标识
S10
第一服务器接收其他设备发送的调用第一服务的第一调用请求，所述第一调用请求中包含第一安全标识；其中，所述第一安全标识用于验证所述第一调用请求的合法性
S11
根据所述第一调用请求中包含的第一安全标识，获取与所述第一安全标识对应的第一用户信息
S12
如果所述第一用户信息满足预设的规则，执行所述第一调用请求
S13

图 4

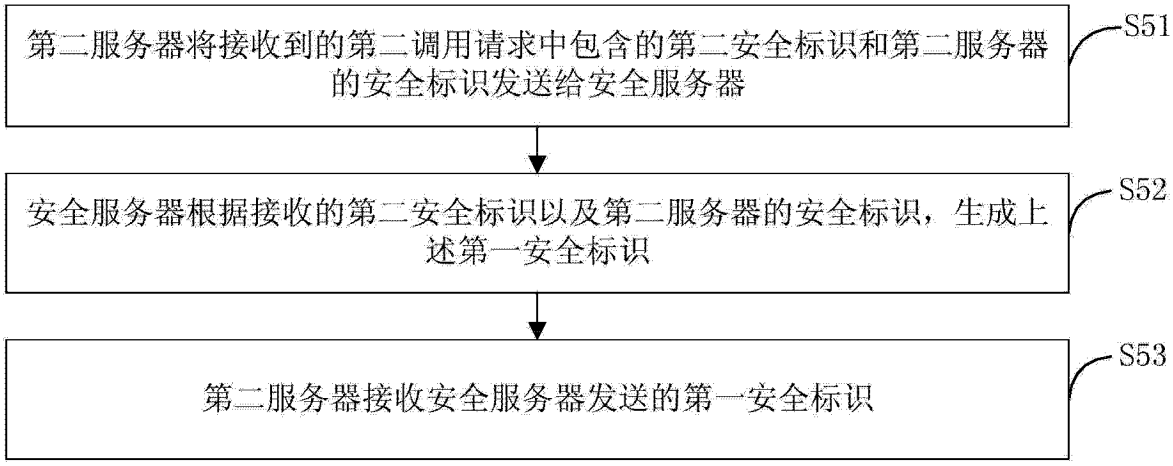

第二服务器将接收到的第二调用请求中包含的第二安全标识和第二服务器的安全标识发送给安全服务器
S51
安全服务器根据接收的第二安全标识以及第二服务器的安全标识，生成上述第一安全标识
S52
第二服务器接收安全服务器发送的第一安全标识
S53

图 5

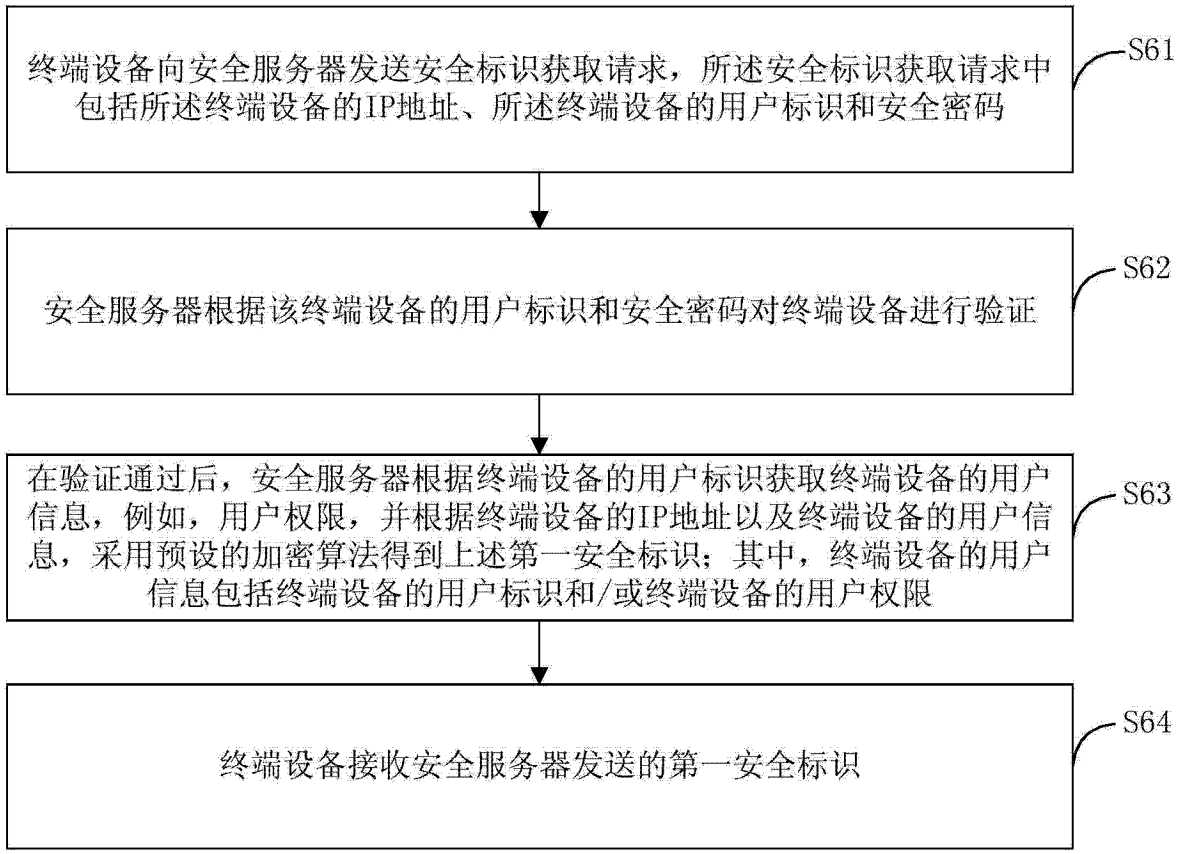

终端设备向安全服务器发送安全标识获取请求，所述安全标识获取请求中包括所述终端设备的IP地址、所述终端设备的用户标识和安全密码
S61
安全服务器根据该终端设备的用户标识和安全密码对终端设备进行验证
S62
在验证通过后，安全服务器根据终端设备的用户标识获取终端设备的用户信息，例如，用户权限，并根据终端设备的IP地址以及终端设备的用户信息，采用预设的加密算法得到上述第一安全标识；其中，终端设备的用户信息包括终端设备的用户标识和/或终端设备的用户权限
S63
终端设备接收安全服务器发送的第一安全标识
S64

图 6

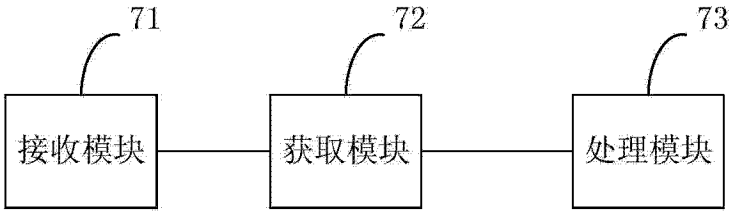


图 7

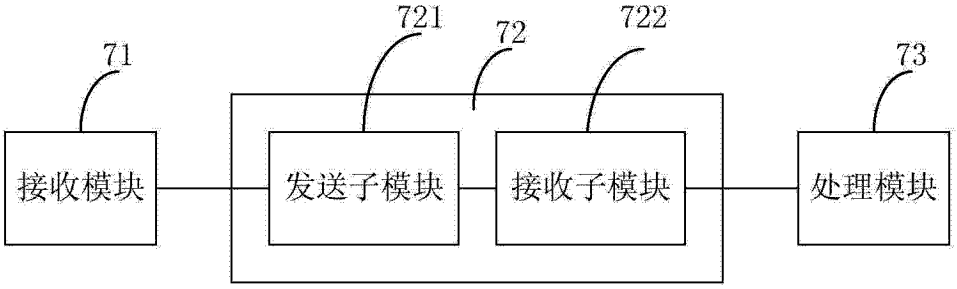


图 8a

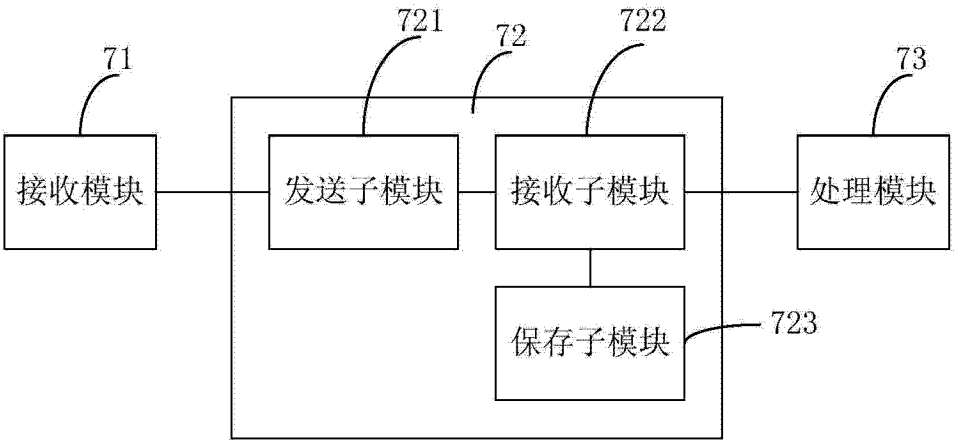


图 8b

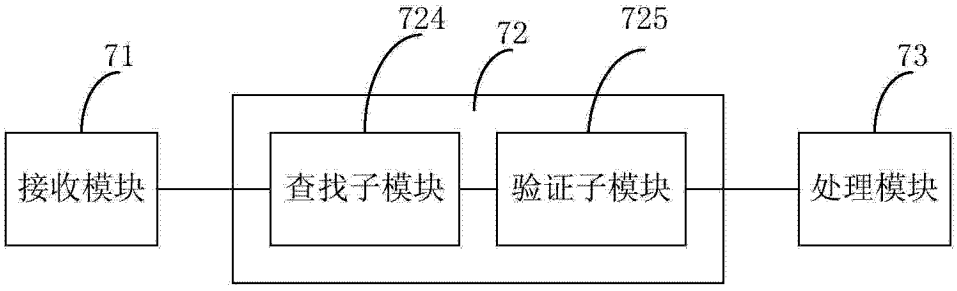


图 8c

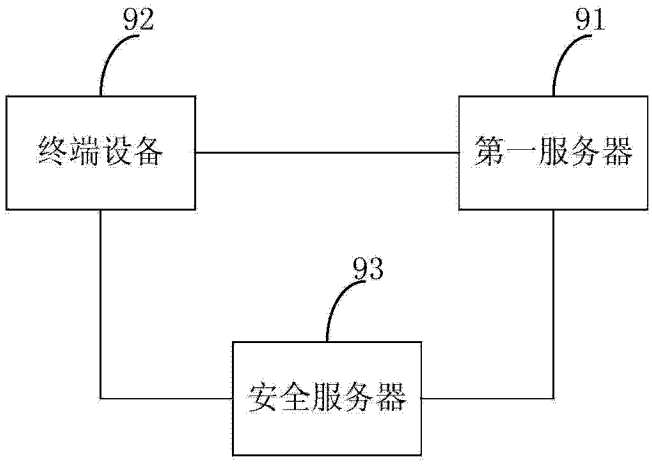


图 9

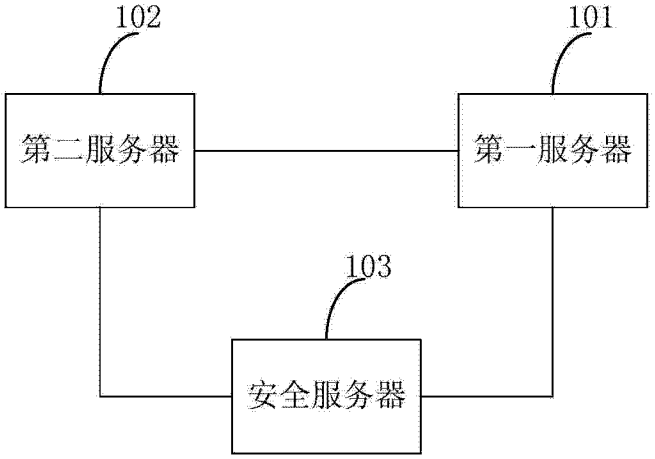


图 10