



(12)发明专利申请

(10)申请公布号 CN 106657098 A

(43)申请公布日 2017. 05. 10

(21)申请号 201611248409.0

(22)申请日 2016.12.29

(71)申请人 郑州云海信息技术有限公司

地址 450018 河南省郑州市郑东新区心怡路278号16层1601室

(72)发明人 史书伟

(74)专利代理机构 北京集佳知识产权代理有限公司 11227

代理人 罗满

(51) Int. Cl.

H04L 29/06(2006.01)

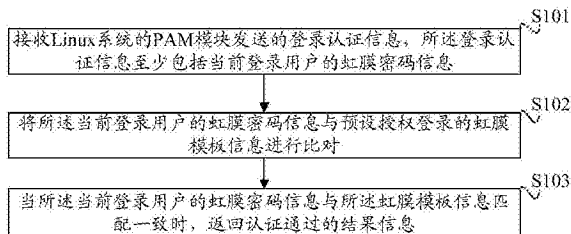
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种登录Linux操作系统的认证方法、装置以及系统

(57)摘要

本发明公开了一种登录Linux操作系统的认证方法及装置,通过接收Linux系统的PAM模块发送的登录认证信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;在当前登录用户的虹膜密码信息与虹膜模板信息匹配一致时,返回认证通过的结果信息。本发明基于PAM模块的可热插拔及易用性,实现了登录Linux操作系统的认证。PAM模块可动态加载验证模块,大大提高了验证的灵活性。另外,本申请采用虹膜认证技术的生物识别特性,实现了用户的身份认证。通过PAM本身的易用性及虹膜技术的唯一性,确保了登录操作系统的安全性。此外,本发明还提供了一种具有上述技术优点的登录Linux操作系统的认证系统。



1. 一种登录Linux操作系统的认证方法,其特征在于,包括:

接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;

将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;

当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。

2. 如权利要求1所述的登录Linux操作系统的认证方法,其特征在于,在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还包括:

当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,根据预设策略确定所述当前登录用户的操作权限信息。

3. 如权利要求2所述的登录Linux操作系统的认证方法,其特征在于,所述登录认证信息还包括访问端的IP地址信息。

4. 如权利要求3所述的登录Linux操作系统的认证方法,其特征在于,所述根据预设策略确定所述当前登录用户的操作权限信息包括:

根据当前登录时间信息判断当前登录是否处于预设可访问时间段内;

根据所述IP地址信息判断当前访问端的IP地址是否具有访问操作权限。

5. 如权利要求1至4任一项所述的登录Linux操作系统的认证方法,其特征在于,在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还包括:

当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配不一致时,返回认证错误的结果信息。

6. 如权利要求5所述的登录Linux操作系统的认证方法,其特征在于,所述接收Linux系统的PAM模块发送的登录认证信息包括:

接收经过加密处理的所述登录认证信息,对所述登录认证信息进行解析,确定虹膜密码信息。

7. 一种登录Linux操作系统的认证装置,其特征在于,包括:

接收模块,用于接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;

认证模块,用于将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。

8. 一种登录Linux操作系统的认证系统,其特征在于,包括:

虹膜扫描器,用于采集当前登录用户的虹膜信息,并将所述虹膜信息进行编码,生成虹膜密码信息;

Linux操作系统客户端,用于将包含所述虹膜密码信息的登录认证信息发送到虹膜认证服务器;

所述虹膜认证服务器,用于接收所述虹膜密码信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,生成认证通过的结果信息。

9. 如权利要求8所述的登录Linux操作系统的认证系统,其特征在于,所述登录认证信息还包括访问端的IP地址信息。

10. 如权利要求9所述的登录Linux操作系统的认证系统,其特征在于,所述Linux操作系统客户端还用于对所述登录认证信息进行加密,将加密后的信息发送到所述虹膜认证服务器。

一种登录Linux操作系统的认证方法、装置以及系统

技术领域

[0001] 本发明涉及安全认证技术领域,特别是涉及一种登录Linux操作系统的认证方法、装置以及系统。

背景技术

[0002] 身份认证技术是信息安全理论与技术的一个重要方面,它是系统安全的第一道防线,用于限制非法用户访问受限的系统资源,是一切安全机制的基础,这也就使之成为黑客攻击的主要目标。因此使用一个强健有效的身份认证系统对于网络安全有着非同寻常的意义。

[0003] 就国内外身份认证技术的发展情况来看,最传统的身份认证方式是帐号—固定密码方式。但是传统的这种方式容易被窃取与破解,安全性较低。

[0004] 新兴的身份认证方式包括:生物特征识别法、声音认证法等。在生物特征识别技术中,人类眼睛的虹膜与手指纹一样,是独一无二的。正因为这样英国剑桥大学的约翰·多曼博士便发明了虹膜身份测定技术。简单地说,虹膜测定技术是将虹膜的外观特征转化为512比特的虹膜密码,再储存在模板内备作确认。一个虹膜大约有266个单位的读取点,而其他传统生物测定技术只能读取13-16个单位。这肯定了虹膜测定的精确程度。此外,使用此技术非常方便,扫描过程只约1分钟。现时,英美已开始把这种身份确认技术用于银行提款机。只在提款机上安装虹膜测定相机,银行便能瞬间确认使用者的身份,保证使用者的密码无法被窃取。

[0005] 鉴于此,提供一种基于虹膜技术的登录Linux操作系统的认证方法、装置以及系统是非常有必要的。

发明内容

[0006] 本发明的目的是提供一种登录Linux操作系统的认证方法、装置以及系统,用于解决传统采用账户密码登录认证的方式安全性较低的问题。

[0007] 为解决上述技术问题,本发明提供一种登录Linux操作系统的认证方法,包括:

[0008] 接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;

[0009] 将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;

[0010] 当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。

[0011] 可选地,在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还包括:

[0012] 当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,根据预设策略确定所述当前登录用户的操作权限信息。

[0013] 可选地,所述登录认证信息还包括访问端的IP地址信息。

- [0014] 可选地,所述根据预设策略确定所述当前登录用户的操作权限信息包括:
- [0015] 根据当前登录时间信息判断当前登录是否处于预设可访问时间段内;
- [0016] 根据所述IP地址信息判断当前访问端的IP地址是否具有访问操作权限。
- [0017] 可选地,在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还包括:
- [0018] 当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配不一致时,返回认证错误的结果信息。
- [0019] 可选地,所述接收Linux系统的PAM模块发送的登录认证信息包括:
- [0020] 接收经过加密处理的所述登录认证信息,对所述登录认证信息进行解析,确定虹膜密码信息。
- [0021] 本发明还提供了一种登录Linux操作系统的认证装置,包括:
- [0022] 接收模块,用于接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;
- [0023] 认证模块,用于将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。
- [0024] 本发明还提供了一种登录Linux操作系统的认证系统,包括:
- [0025] 虹膜扫描器,用于采集当前登录用户的虹膜信息,并将所述虹膜信息进行编码,生成虹膜密码信息;
- [0026] Linux操作系统客户端,用于将包含所述虹膜密码信息的登录认证信息发送到虹膜认证服务器;
- [0027] 所述虹膜认证服务器,用于接收所述虹膜密码信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,生成认证通过的结果信息。
- [0028] 可选地,所述登录认证信息还包括访问端的IP地址信息。
- [0029] 可选地,所述Linux操作系统客户端还用于对所述登录认证信息进行加密,将加密后的信息发送到所述虹膜认证服务器。
- [0030] 本发明所提供的登录Linux操作系统的认证方法及装置,通过接收Linux系统的PAM模块发送的登录认证信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;在当前登录用户的虹膜密码信息与虹膜模板信息匹配一致时,返回认证通过的结果信息。本发明基于PAM模块的可热插拔及易用性,实现了登录Linux操作系统的认证。PAM模块可动态加载验证模块,可以按需要动态的对验证的内容进行变更,大大提高了验证的灵活性。另外,本申请采用虹膜认证技术的生物识别特性,实现了用户的身份认证。通过PAM本身的易用性及虹膜技术的唯一性,确保了登录操作系统的安全性。此外,本发明还提供了一种具有上述技术优点的登录Linux操作系统的认证系统。

附图说明

[0031] 为了更清楚的说明本发明实施例或现有技术的技术方案,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的介绍,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。

[0032] 图1为本发明所提供的登录Linux操作系统的认证方法的一种具体实施方式的流程图;

[0033] 图2为本发明所提供的登录Linux操作系统的认证方法的另一种具体实施方式的流程图;

[0034] 图3为本发明实施例提供的登录Linux操作系统的认证装置的结构框图;

[0035] 图4为本发明所提供的认证系统的示意图。

具体实施方式

[0036] 为了使本技术领域的人员更好地理解本发明方案,下面结合附图和具体实施方式对本发明作进一步的详细说明。显然,所描述的实施例仅仅是本发明一部分实施例,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。

[0037] 本发明所提供的登录Linux操作系统的认证方法的一种具体实施方式的流程图如图1所示,该方法包括:

[0038] 步骤S101:接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;

[0039] 需要说明的是,本发明可以具体应用于虹膜认证服务器。该虹膜认证服务器通过网络设备与Linux操作系统客户端相连,在Linux操作系统客户端设置虹膜采集器,对登录用户的虹膜图像进行采集。

[0040] 登录认证信息可以具体包含当前登录用户的虹膜密码信息,具体可以为当用户登录Linux系统中,按照Linux系统端设置认证规则,采用虹膜采集器采集当前登录用户的虹膜信息,进行编码后生成虹膜密码信息。Linux系统的PAM将虹膜密码信息发送至本实施例中虹膜认证服务器,以进行认证。

[0041] 登录认证信息还可以包括其他信息,例如访问端的IP地址等其他信息。并且为了进一步提高系统认证的安全性,登录认证信息还可以做加密处理再进行传输,以免明文发送导致信息泄露情况的发生。虹膜认证服务器在接收到登录认证信息后,对登录认证信息进行解密,并且解析出虹膜密码信息,或对应的访问端的IP地址信息。

[0042] 步骤S102:将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;

[0043] 步骤S103:当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。

[0044] 虹膜认证服务器将解析得到的虹膜密码信息与预设授权登录的虹膜模板信息进行比对。虹膜模板信息为预先建立的可对Linux系统进行访问的已授权用户的虹膜密码信息,只有在当前登录用户的虹膜密码信息与虹膜模板信息中的至少一个匹配一致时,才能认为当前登录用户的虹膜密码信息合法,即当前登录用户为授权用户。认证通过后,用户可登录Linux操作系统。

[0045] 本发明所提供的登录Linux操作系统的认证方法,通过接收Linux系统的PAM模块

发送的登录认证信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对;在当前登录用户的虹膜密码信息与虹膜模板信息匹配一致时,返回认证通过的结果信息。本发明基于PAM模块的可热插拔及易用性,实现了登录Linux操作系统的认证。PAM模块可动态加载验证模块,可以按需要动态的对验证的内容进行变更,大大提高了验证的灵活性。另外,本申请采用虹膜认证技术的生物识别特性,实现了用户的身份认证。通过PAM本身的易用性及虹膜技术的唯一性,确保了登录操作系统的安全性。

[0046] 在当前登录用户的虹膜密码信息与虹膜模板信息匹配一致时,即当前用户为授权用户时,可以为不同的授权用户分别设置不同的操作权限。在上述实施例的基础上,本发明实施例在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还可以进一步包括:

[0047] 当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,根据预设策略确定所述当前登录用户的操作权限信息。

[0048] 具体地,可以根据当前登录时间信息判断当前登录是否处于预设可访问时间段内;根据所述IP地址信息判断当前登录的IP地址是否具有访问操作权限。

[0049] 例如,系统预设第一用户只有在上班时间才具有访问Linux操作系统,这样当用户当前访问时间为下午8点,即不在上班时间时即便用户为授权用户也不能够访问Linux操作系统。权限判断条件除了包括上述时间信息,还可以包括日期信息,或者上述访问端的IP地址信息,这均不影响本发明的实现。

[0050] 此外,在上述任一实施例的基础上,本发明所提供的登录Linux操作系统的认证方法中,在所述将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比对之后还包括:当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配不一致时,返回认证错误的结果信息。

[0051] 下面结合具体实施场景,对本发明所提供的登录Linux操作系统的认证方法的另一种具体实施方式进行详细阐述,参照图2,结构设计采用集中式认证管理,所有受控的Linux系统发送信息到虹膜认证服务器统一做认证该方法包括:

[0052] 步骤S201:当用户登陆Linux系统时,按照Linux系统端设置认证规则,使用虹膜扫描仪采集登录用户的虹膜信息并进行编码;

[0053] 在用户登陆Linux操作系统时,由虹膜扫描仪扫描登录者的眼睛虹膜,并把虹膜信息识别点特征采集出来,转换成虹膜密码。

[0054] 步骤S202:Linux系统的PAM处理虹膜信息,把虹膜信息进行加密,再加访问端的IP地址一起通过发送到虹膜认证服务器做认证;

[0055] 虹膜密码及登陆信息通过网络被发送到虹膜认证服务器经行认证,并返回认证信息。

[0056] 步骤S203:虹膜认证服务器接收认证信息,再解析认证信息,得到虹膜密码信息、IP地址信息,解析完毕后,判断该虹膜信息是否合法,如果信息不合法,则返回认证错误信息,如果信息合法,则根据虹膜认证服务器的策略设置判断是否受限(包括当前登陆时间、日期、登陆IP地址等);

[0057] 步骤S204:验证结果返回给Linux操作系统,操作系统解析返回结果。如果认证通过,则进入操作系统;否则认证不通过,则直接弹出错误信息。

[0058] 下面对本发明实施例提供的登录Linux操作系统的认证装置进行介绍,下文描述的登录Linux操作系统的认证装置与上文描述的登录Linux操作系统的认证方法可相互对应参照。

[0059] 图3为本发明实施例提供的登录Linux操作系统的认证装置的结构框图,参照图3登录Linux操作系统的认证装置可以包括:

[0060] 接收模块100,用于接收Linux系统的PAM模块发送的登录认证信息,所述登录认证信息至少包括当前登录用户的虹膜密码信息;

[0061] 认证模块200,用于将所述当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比较;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,返回认证通过的结果信息。

[0062] 本实施例的登录Linux操作系统的认证装置用于实现前述的登录Linux操作系统的认证方法,因此登录Linux操作系统的认证装置中的具体实施方式可见前文中的登录Linux操作系统的认证方法的实施例部分,例如,接收模块100,用于实现上述登录Linux操作系统的认证方法中步骤S101,认证模块200用于实现上述方法中步骤S102和S203,所以,其具体实施方式可以参照相应的各个部分实施例的描述,在此不再赘述。

[0063] 此外,本发明还提供了一种登录Linux操作系统的认证系统,如图4本发明所提供的认证系统的示意图所示,该系统包括:

[0064] 虹膜扫描器,用于采集当前登录用户的虹膜信息,并将所述虹膜信息进行编码,生成虹膜密码信息;

[0065] Linux操作系统客户端,用于将包含所述虹膜密码信息的登录认证信息发送到虹膜认证服务器;

[0066] 所述虹膜认证服务器,用于接收所述虹膜密码信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进行比较;当所述当前登录用户的虹膜密码信息与所述虹膜模板信息匹配一致时,生成认证通过的结果信息。

[0067] 本申请充分利用眼睛虹膜特有的唯一性的特点,在Linux系统的PAM认证过程中,把虹膜外观特征转化的512比特的虹膜密码转发到认证服务器进行认证,认证服务器对密码及认证策略进行判断,返回认证结果,Linux系统显示认证结果或者通过认证进入系统。

[0068] 其中,所述登录认证信息还包括访问端的IP地址信息。虹膜认证服务器用于对虹膜密码进行认证,并对认证用户的访问策略进行判断,包括认证时间,访问端IP地址等。

[0069] 作为一种具体实施方式,上述Linux操作系统客户端还用于对所述登录认证信息进行加密后,发送到所述虹膜认证服务器。

[0070] 虹膜认证服务器端,用于解析Linux系统端发送来的虹膜密码、IP地址等信息;Linux系统端,用于解析认证服务器端发送来的认证结果,包括密码错误、当前时间段禁止登陆等。

[0071] 参照图4,本发明提供的系统的工作过程具体为,虹膜密码首先被录入,然后通过PAM中发送到虹膜认证服务器,再由虹膜认证服务器解析出信息,进行判断。判断完毕后再将认证结果信息返回给操作系统,由操作系统解析出认证结果,判断是否继续进行登录。

[0072] 本发明所提供的登录Linux操作系统的认证系统,通过接收Linux系统的PAM模块发送的登录认证信息,将当前登录用户的虹膜密码信息与预设授权登录的虹膜模板信息进

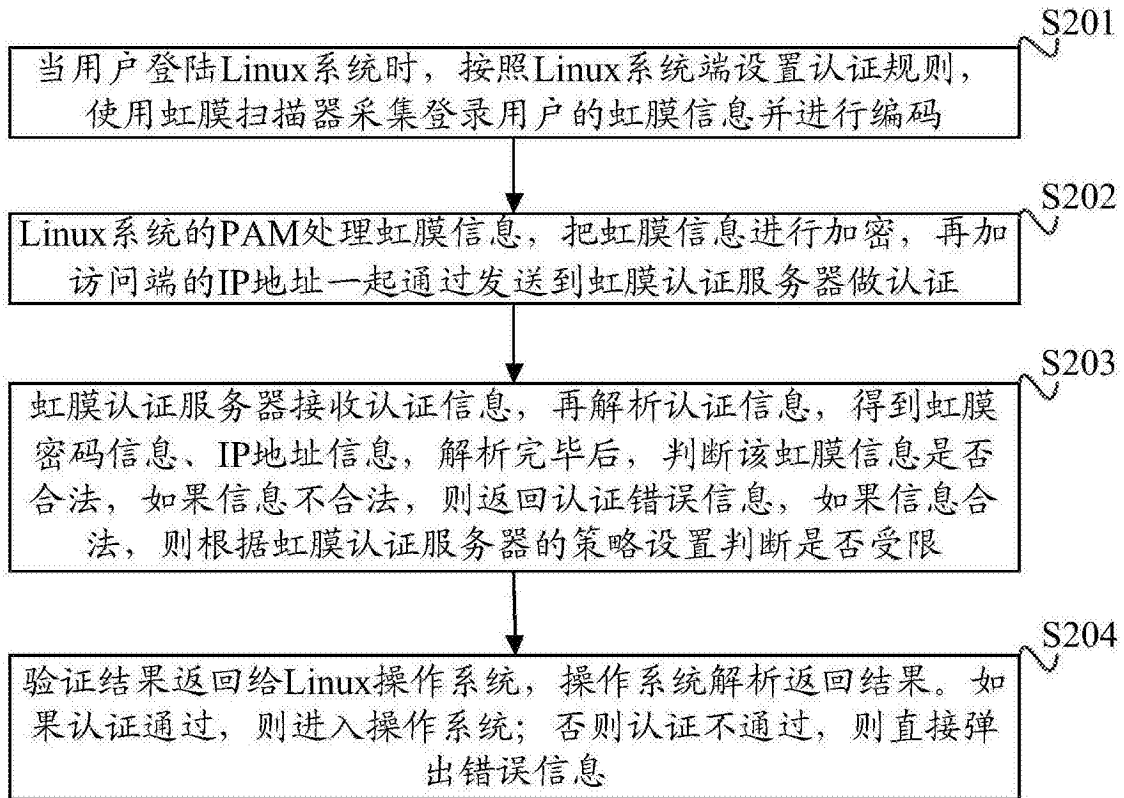
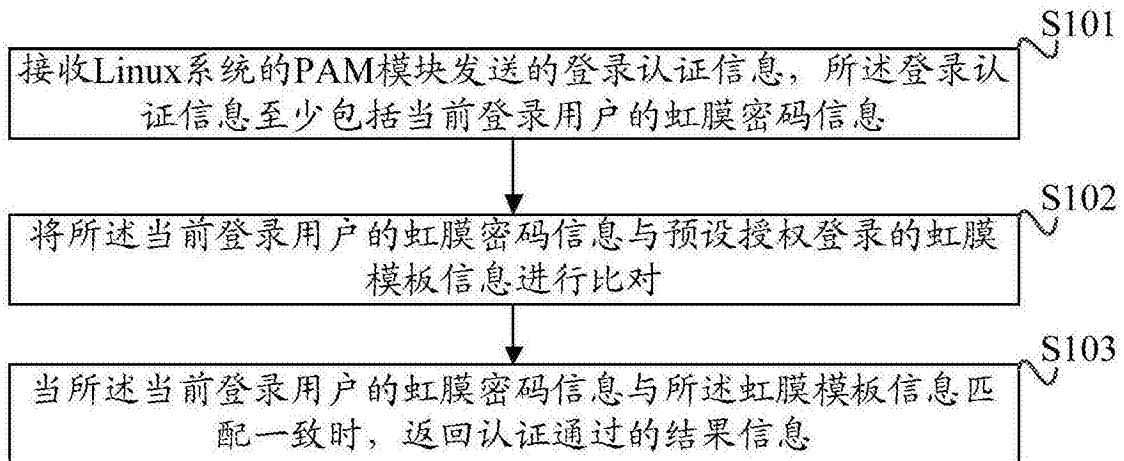
行比对;在当前登录用户的虹膜密码信息与虹膜模板信息匹配一致时,返回认证通过的结果信息。本发明基于PAM模块的可热插拔及易用性,实现了登录Linux操作系统的认证。PAM模块可动态加载验证模块,可以按需要动态的对验证的内容进行变更,大大提高了验证的灵活性。另外,本申请采用虹膜认证技术的生物识别特性,实现用户的身份认证。通过PAM本身的易用性及虹膜技术的唯一性,确保了登录操作系统的安全性。

[0073] 本说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其它实施例的不同之处,各个实施例之间相同或相似部分互相参见即可。对于实施例公开的装置而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0074] 专业人员还可以进一步意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0075] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块,或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0076] 以上对本发明所提供的登录Linux操作系统的认证方法、装置以及系统进行了详细介绍。本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想。应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以对本发明进行若干改进和修饰,这些改进和修饰也落入本发明权利要求的保护范围内。



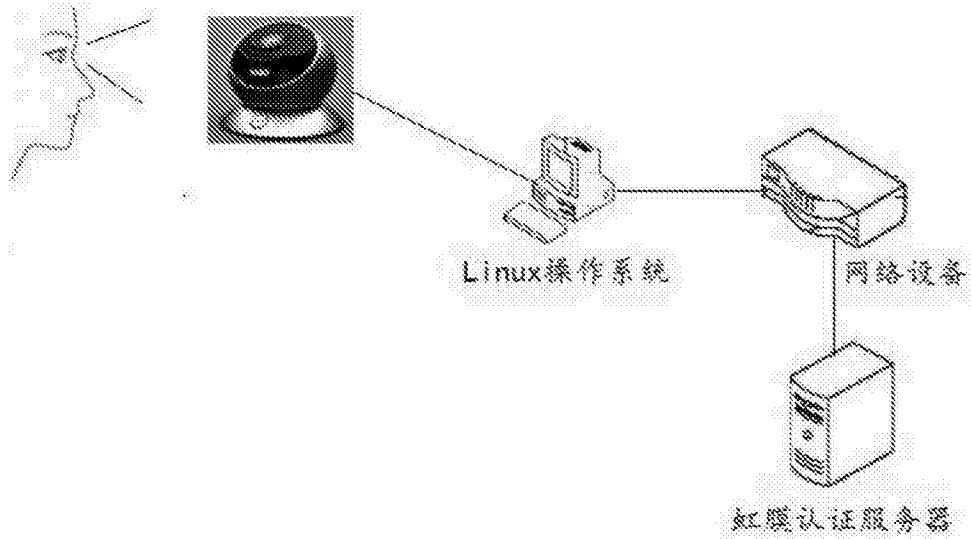


图4