1. 本发明要解决的技术问题是什么，同时说明本发明的目的

本发明专利要解决的技术问题和发明目的如下：

Linux系统下的集中化管理指纹仪登陆认证的方法

现有的LINUX系统认证方式有用户名密码认证/智能卡认证/动态口令认证/USBKey认证/指纹认证等。

用户名/密码是最简单也是最常用的身份认证方法，但是由于用户密码容易忘记或者容易被窃取，因此用户名/密码方式一种是极不安全的身份认证方式。

智能卡认证/动态口令认证/USBKey认证，是现有登陆认证的有效补充，通过附加硬件增加认证功能，提供有效的密码保护。但是缺点是容易被破解，输入口令或者PIN码繁琐，因此有一定的缺陷。

指纹认证，是比较安全的认证方式，与传统身份认证技术相比，生物识别技术具有以下特点：

1. 随身性：指纹生物特征是人体固有的特征，与人体是唯一绑定的，具有随身性。
2. 安全性：人体特征本身就是个人身份的最好证明,满足更高的安全需求。
3. 唯一性：每个人拥有的指纹生物特征各不相同。
4. 稳定性：指纹特征不会随时间等条件的变化而变化。
5. 广泛性：每个人都具有指纹特征。
6. 方便性：指纹识别技术不需记忆密码与携带使用特殊工具，不会遗失。
7. 可采集性：指纹物特征易于测量。

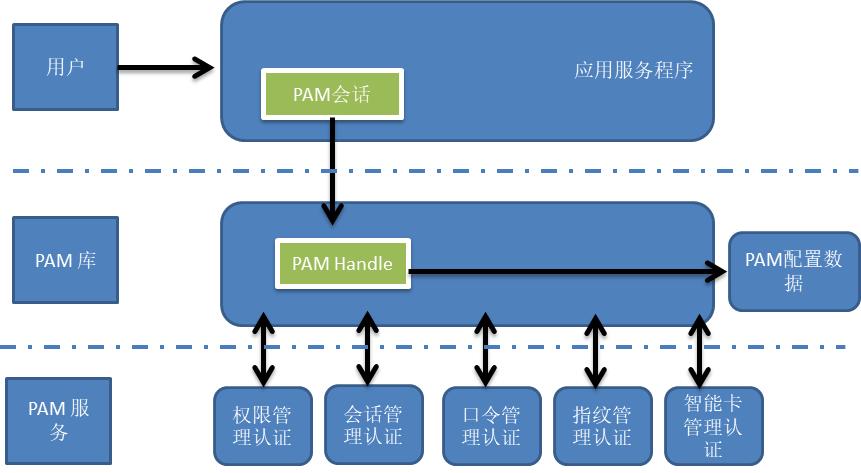
现有的指纹登陆认证方案，一般采取指纹特征保存在指纹仪设备中或者LINUX计算机内部磁盘的方式，存在安全隐患。比如一定磁盘文件丢失或者指纹设备丢失，用户就无法登陆。 同时每台计算机独占一台指纹仪设备，不利于指纹仪设备共享使用。本发明是基于现有指纹登陆认证的一种扩展，采用集中化管理指纹特征数据，保证指纹特征的安全性，并提高指纹仪设备利用率，多个计算机可以共享使用一台指纹仪设备。本发明完全通过软件实现，不依赖具体设备，可极大降低IT系统设备成本同时提高系统安全性。

1. 详细介绍技术背景，并描述已有的与本发明创造最相近似的实现方案
2. Linux PAM认证机制简介

Linux 最初的认证采取验证用户密码的方式进行认证。但是随着技术的发展，新的认证方式不断涌现，比如采用智能卡认证机制。以前这些认证方式的通病是，提供认证服务的程序，都要开发自己特有的代码进行编译，因为程序也要为特定的认证接口开发代码并重新编译。

PAM认证机制就是解决这种问题，通过制定一套标准的权限认证协议，使权限认证服务提供方（比如密码认证、指纹认证）与权限认证使用方（比如桌面服务、FTP应用等）各自分离开发，互不影响。权限认证服务方与权限认证使用方，通过公用的API接口进行调用，用户可以灵活配置应用程序的权限认证服务。

1. Linux PAM 框架



如上图所示，PAM可插拔权限认证模式， 采用集中认证的方式。 其中应用服务程序，比如远程登陆或者FTP服务，通过PAM库启动一个会话，根据管理员的PAM配置数据决定调用那些权限认证服务。

1. 应用服务使用PAM权限认证

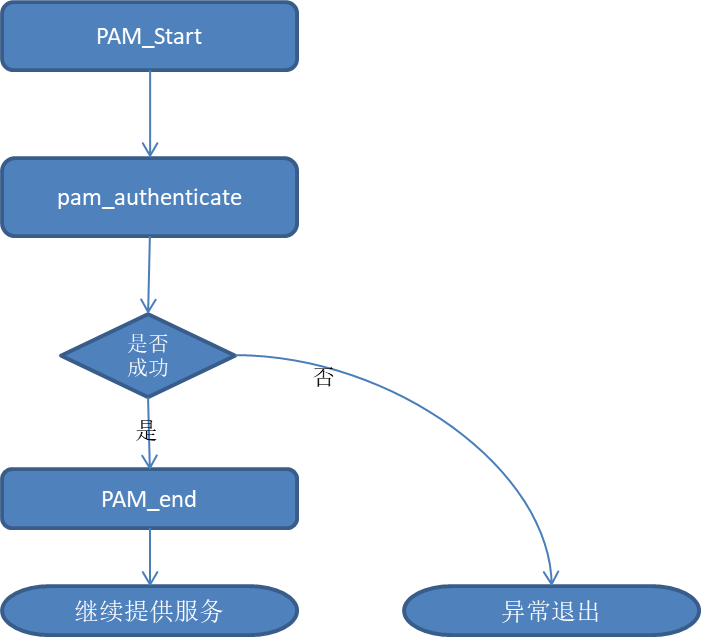
每个使用PAM认证的应用程序都以pam\_start开始，pam\_end结束。PAM还提供了pam\_get\_item和pam\_set\_item共享有关认证会话的某些公共信息，例如用户名，服务名，密码和会话函数。应用程序在调用了pam\_start ()后也能够用这些APIs来改变状态信息。实际做认证工作包含以下步骤：

认证管理--包括pam\_authenticate ()函数认证用户。

账号管理--包括pam\_acc\_mgmt ()检查认证的用户是否可以访问他们的账户。

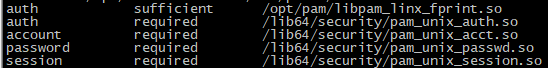
会话管理--包括pam\_open\_session ()和pam\_close\_session ()函数用来管理会话和记账。口令管理--包括pam\_chauthok ()函数用来改变密码。

以下是一个典型应用程序使用PAM的过程：



1. PAM库工作机制及其PAM配置数据

PAM函数库通过pam\_start启动会话，PAM配置数据决定了需要启动的鉴权认证服务以及启动参数。下图是一个典型的PAM配置文件格式：



配置文件包含信息:type/control/module-path/module-arguments , 即认证类型/控制方式/模块路径/模块参数。

认证类型分为：权限/账户/密码/会话类型

控制方式分为：required必要类型；sufficient 满足一种类型（满足本模块认证，后续认证可以忽略）；

1. PAM认证服务工作机制

PAM认证服务模块需要提供PAM标准接口，其中最重要的是pam\_sm\_authenticate函数接口，该函数必须完成认证需要执行的步骤。

模块各自要实现的函数如下表所示：

|  |  |  |
| --- | --- | --- |
| 模块类型 | 要实现的函数 | 函数功能 |
| 认证管理 | pam\_sm\_authenticate | 认证用户 |
| pam\_sm\_setcred | 设置用户证书 |
| 账号管理 | pam\_sm\_acct\_mgmt | 帐号管理 |
| 会话管理 | int pam\_sm\_open\_session | 打开会话 |
| int pam\_sm\_close\_session | 关闭会话 |
| 口令管理 | pam\_sm\_chauthtok | 设置口令 |

也就是通过实现不同的pam\_sm\_authenticate函数接口，就可以完成不同的认证用户过程。 比如用户密码认证服务只需要比对用户输入的密码是否正确，指纹认证服务则通过比对用户指纹特征与系统保存指纹特征是否匹配。

三、本发明创造技术方案的详细阐述，应该结合流程图、原理框图、电路图、时序图进行说明