



(12) 发明专利申请

(10) 申请公布号 CN 105450672 A

(43) 申请公布日 2016. 03. 30

(21) 申请号 201610005678. 8

(22) 申请日 2016. 01. 05

(71) 申请人 上海大之商科技发展股份有限公司

地址 201400 上海市奉贤区望园路 2066 弄 6
幢 2 层 240 室

(72) 发明人 徐杰 钱昌宏

(74) 专利代理机构 北京青松知识产权代理事务
所（特殊普通合伙） 11384

代理人 郑青松

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

H04L 9/08(2006. 01)

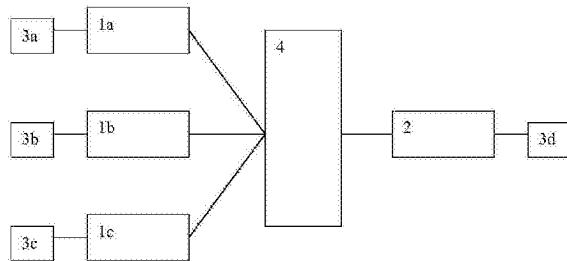
权利要求书2页 说明书5页 附图1页

(54) 发明名称

一种财务数据的内部网络安全传输方法与系
统

(57) 摘要

本发明提供了一种财务数据的内部网络安全
传输方法和系统，所述系统包括多个财务数据处
理终端，每个处理终端都配有与之唯一对应的身
份令牌，其中存储有代表所连接终端的唯一身份
识别码，以及管理服务器，管理服务器接生成表示
汇总财务数据的任务的任务密码，任务密码存储
到与较高级终端连接的身份令牌中，较高级终端
读取到身份令牌中存储的任务密码后，用户才能
读取或处理关于该任务的财务数据。采用此类方
式，可以有效防止财务数据被泄露或篡改，提高了
内部网络的安全性。



1. 一种财务数据的内部网络安全传输系统,其特征在于,包括:多个财务数据处理终端,所述处理终端包括设置了终端等级的较高级终端和较低级终端,每个处理终端都配与之唯一对应的身份令牌,身份令牌与处理终端连接,其中存储有代表所连接终端的唯一身份识别码,以及管理服务器,多个财务数据处理终端以及管理服务器通过内部网络互相连接;

较高级终端在当希望汇总财务数据时,用户将其对应的身份令牌与较高级终端连接,读取身份令牌中保存的身份识别码,确认当前用户有权限操作该较高级终端之后,较高级终端对汇总财务数据的任务进行任务等级确认,之后将包括任务等级的财务数据接收请求和自身身份识别码发送至管理服务器;

管理服务器在接收到财务数据接收请求后,将该请求向所有较低级终端广播;

较低级终端接收到广播消息后,检查自身是否存储有所请求的财务数据,若有,待各自的操作用户将与之对应的管理令牌连接到较低级终端进行操作时,对用户进行提示,经用户操作后,各个较低级终端将管理令牌中保存的身份识别码连同自身存储的财务数据发送到管理服务器,发送完毕后,较低级终端根据财务数据接收请求中包含的任务等级,确定是否删除本机存储的财务数据;

管理服务器接收到较低级终端分别发送的财务数据和相应的身份识别码后,根据财务数据发送方和接收方的身份识别码,生成表示汇总财务数据的任务的任务密码,该任务密码根据以下的方式生成:对于每一终端,管理服务器中都存储有与之对应的6位身份暗码,管理服务器根据任务所涉及的所有终端,读取所有相应身份暗码,确定身份暗码的数量n,生成位数为(6*n+8)位的任务初始码,其中该任务初始码从第1位开始,每6位都和某一终端的身份暗码相同,最后8位则为一串随机字符,对于(6*n+8)位的任务初始码,采用整体移位加密方式生成任务密码,即将每位字符均向左或向右移动若干位,右边或左边空出的位数由左边或右边多出的字符补满,管理服务器将较低级终端分别发送的财务数据设置为通过任务密码才能读取,并将其与生成的任务密码发送给较高级终端;

较高级终端接收到管理服务器发送的较低级终端的财务数据和生成的任务密码后,将财务数据存储于较高级终端内,将任务密码存储到与较高级终端连接的身份令牌中,用于之后用户通过身份令牌连接到较高级终端后,较高级终端读取到身份令牌中存储的任务密码后,用户才能读取或处理关于该任务的财务数据。

2. 一种如权利要求1所述的财务数据的内部网络安全传输系统,其特征在于,当企业需要多层次上报财务数据时,设置三级以上的处理终端,进行多层次扩展。

3. 一种如权利要求1所述的财务数据的内部网络安全传输系统,其特征在于,其中,当任务等级大于终端等级时,处理终端在将自身存储的财务数据发送到管理服务器之后,自动将该财务数据删除;当任务等级小于等于终端等级时,继续保存该财务数据。

4. 一种财务数据的内部网络安全传输方法,其特征在于,包括如下步骤:

S1,较高级终端在当希望汇总财务数据时,用户将其对应的身份令牌与较高级终端连接,读取身份令牌中保存的身份识别码,确认当前用户有权限操作该较高级终端之后,较高级终端对汇总财务数据的任务进行任务等级确认,之后将包括任务等级的财务数据接收请求和自身身份识别码发送至管理服务器;

S2,管理服务器在接收到财务数据接收请求后,将该请求向所有较低级终端广播;较低

级终端接收到广播消息后,检查自身是否存储有所请求的财务数据,若有,待各自的操作用户将与之对应的管理令牌连接到较低级终端进行操作时,对用户进行提示,经用户操作后,各个较低级终端将管理令牌中保存的身份识别码连同自身存储的财务数据发送到管理服务器,发送完毕后,较低级终端根据财务数据接收请求中包含的任务等级,确定是否删除本机存储的财务数据;

S3,管理服务器接收到较低级终端分别发送的财务数据和相应的身份识别码后,根据财务数据发送方和接收方的身份识别码,生成表示汇总财务数据的任务的任务密码,该任务密码根据以下的方式生成:对于每一终端,管理服务器中都存储有与之对应的6位身份暗码,管理服务器根据任务所涉及的所有终端,读取所有相应身份暗码,确定身份暗码的数量n,生成位数为(6*n+8)位的任务初始码,其中该任务初始码从第1位开始,每6位都和某一终端的身份暗码相同,最后8位则为一串随机字符,对于(6*n+8)位的任务初始码,采用整体移位加密方式生成任务密码,即将每位字符均向左或向右移动若干位,右边或左边空出的位数由左边或右边多出的字符补满,管理服务器将较低级终端分别发送的财务数据设置为通过任务密码才能读取,并将其与生成的任务密码发送给较高级终端;

S4,较高级终端接收到管理服务器发送的较低级终端的财务数据和生成的任务密码后,将财务数据存储于较高级终端内,将任务密码存储到与较高级终端连接的身份令牌中,用于之后用户通过身份令牌连接到较高级终端后,较高级终端读取到身份令牌中存储的任务密码后,用户才能读取或处理关于该任务的财务数据。

一种财务数据的内部网络安全传输方法与系统

技术领域

[0001] 本发明涉及网络安全技术领域,尤其涉及一种财务数据的内部网络安全传输方法与系统。

背景技术

[0002] 随着我国国民经济的飞速发展,国内各行各业的生产经营水平也在高速进步,各种大型企业的数量正在快速攀升。对于这些大型企业来说,随着世界范围内信息化进程的加快,财务数据已经成为关系到自身过去、现在和未来的重要数据,在企业的数据挖掘、日常管理、战略规划等各个方面都发挥着重要作用,是企业的一种重要资产。

[0003] 为了保证财务数据的安全,越来越多的企业选择在企业内部构建独立于互联网之外的专用网络,定期对该财务数据内部网络进行病毒和木马的查杀,同时对该网络的访问权限做出严格的规定,以期能够及时发现并纠正安全隐患,保证被允许的用户浏览和处理财务数据。采用这种方式构建起专用网络,确实能够基本上杜绝财务数据通过互联网被窃取。然而,重要的高密性财务数据往往代表着数以亿计的商业吸引力,仍有可能通过有权限访问该专用网络的人员被泄密。

[0004] 现有技术中,通过监视财务数据文件的读取和运行记录,以及通过对工作终端不定期截屏等手段来形成安全威慑,并查找财务数据如何在内部网络被窃取。这种方式需要对每份财务数据文件的生成、读取、保存、修改、复制、移动、删除等操作都进行追踪,还需要设置多样的外部设备,对内部网络的软件和硬件组成以及日常的信合消耗造成了较高的负担。另外,这种方式还会将员工置于被监视的位置,给员工造成强烈的不信任感。因此,需要一种效率更高、花费更少、员工体验更好的财务数据的内部网络安全传输方法与系统。

发明内容

[0005] 为了克服上述现有技术存在的缺陷,本发明提供了一种财务数据的内部网络安全传输系统,其特征在于,包括:多个财务数据处理终端,所述处理终端包括设置了终端等级的较高级终端和较低级终端,每个处理终端都配有与之唯一对应的身份合牌,身份合牌与处理终端连接,其中存储有代表所连接终端的唯一身份识别码,以及管理服务器,多个财务数据处理终端以及管理服务器通过内部网络互相连接;较高级终端在当希望汇总财务数据时,用户将其对应的身份合牌与较高级终端连接,读取身份合牌中保存的身份识别码,确认当前用户有权限操作该较高级终端之后,较高级终端对汇总财务数据的任务进行任务等级确认,之后将包括任务等级的财务数据接收请求和自身身份识别码发送至管理服务器;管理服务器在接收到财务数据接收请求后,将该请求向所有较低级终端广播;较低级终端接收到广播消息后,检查自身是否存储有所请求的财务数据,若有,待各自的操作用户将与之对应的管理合牌连接到较低级终端进行操作时,对用户进行提示,经用户操作后,各个较低级终端将管理合牌中保存的身份识别码连同自身存储的财务数据发送到管理服务器,发送完毕后,较低级终端根据财务数据接收请求中包含的任务等级,确定是否删除本机存储的

财务数据；管理服务器接收到较低级终端分别发送的财务数据和相应的身份识别码后，根据财务数据发送方和接收方的身份识别码，生成表示汇总财务数据的任务的任务密码，该任务密码根据以下的方式生成：对于每一终端，管理服务器中都存储有与之对应的6位身份暗码，管理服务器根据任务所涉及的所有终端，读取所有相应身份暗码，确定身份暗码的数量n，生成位数为(6*n+8)位的任务初始码，其中该任务初始码从第1位开始，每6位都和某一终端的身份暗码相同，最后8位则为一串随机字符，对于(6*n+8)位的任务初始码，采用整体移位加密方式生成任务密码，即将每位字符均向左或向右移动若干位，右边或左边空出的位数由左边或右边多出的字符补满，管理服务器将较低级终端分别发送的财务数据设置为通过任务密码才能读取，并将其与生成的任务密码发送给较高级终端；较高级终端接收到管理服务器发送的较低级终端的财务数据和生成的任务密码后，将财务数据存储于较高级终端内，将任务密码存储到与较高级终端连接的身份合牌中，用于之后用户通过身份合牌连接到较高级终端后，较高级终端读取到身份合牌中存储的任务密码后，用户才能读取或处理关于该任务的财务数据。

[0006] 进一步地，上述的财务数据的内部网络安全传输系统，其特征在于，当企业需要多层级上报财务数据时，设置三级以上的处理终端，进行多层次扩展。

[0007] 进一步地，上述的财务数据的内部网络安全传输系统，其特征在于，其中，当任务等级大于终端等级时，处理终端在将自身存储的财务数据发送到管理服务器之后，自动将该财务数据删除；当任务等级小于等于终端等级时，继续保存该财务数据。

[0008] 本发明同样提供了一种财务数据的内部网络安全传输方法，其特征在于，包括如下步骤：S1，较高级终端在当希望汇总财务数据时，用户将其对应的身份合牌与较高级终端连接，读取身份合牌中保存的身份识别码，确认当前用户有权限操作该较高级终端之后，较高级终端对汇总财务数据的任务进行任务等级确认，之后将包括任务等级的财务数据接收请求和自身身份识别码发送至管理服务器；S2，管理服务器在接收到财务数据接收请求后，将该请求向所有较低级终端广播；较低级终端接收到广播消息后，检查自身是否存储有所请求的财务数据，若有，待各自的操作用户将与之对应的管理合牌连接到较低级终端进行操作时，对用户进行提示，经用户操作后，各个较低级终端将管理合牌中保存的身份识别码连同自身存储的财务数据发送到管理服务器，发送完毕后，较低级终端根据财务数据接收请求中包含的任务等级，确定是否删除本机存储的财务数据；S3，管理服务器接收到较低级终端分别发送的财务数据和相应的身份识别码后，根据财务数据发送方和接收方的身份识别码，生成表示汇总财务数据的任务的任务密码，该任务密码根据以下的方式生成：对于每一终端，管理服务器中都存储有与之对应的6位身份暗码，管理服务器根据任务所涉及的所有终端，读取所有相应身份暗码，确定身份暗码的数量n，生成位数为(6*n+8)位的任务初始码，其中该任务初始码从第1位开始，每6位都和某一终端的身份暗码相同，最后8位则为一串随机字符，对于(6*n+8)位的任务初始码，采用整体移位加密方式生成任务密码，即将每位字符均向左或向右移动若干位，右边或左边空出的位数由左边或右边多出的字符补满，管理服务器将较低级终端分别发送的财务数据设置为通过任务密码才能读取，并将其与生成的任务密码发送给较高级终端；S4，较高级终端接收到管理服务器发送的较低级终端的财务数据和生成的任务密码后，将财务数据存储于较高级终端内，将任务密码存储到与较高级终端连接的身份合牌中，用于之后用户通过身份合牌连接到较高级终端后，较高

级终端读取到身份合牌中存储的任务密码后,用户才能读取或处理关于该任务的财务数据。

附图说明

[0009] 图1为本发明的财务数据的内部网络安全传输系统的组成框图。

[0010] 图2为本发明的财务数据的内部网络安全传输方法的流程图。

具体实施方式

[0011] 下面通过实施例,并结合附图,对本发明的技术方案做进一步具体的说明。

[0012] 通常而言,生成财务数据的终端将初始数据上报到高一级的终端进行汇总,高一级的终端再将汇总后的数据上报到更高一级的终端进一步汇总,以此类推,通过层级上报,最终将全面数据展现给企业决策人。例如,某汽车企业,各个4S店的终端将销售数据上报至销售汇总终端,销售汇总终端连同原材料采购汇总终端、广告汇总终端、人力资源汇总终端等将各类型财务数据上报给决策终端,供企业决策人进行决策。

[0013] 如图1所示,本发明所述的一种财务数据的内部网络安全传输系统中,列出了层级上报中的一级,包括:多个财务数据处理终端1a-1c、2等,其中处理终端被赋予不同的等级,例如图1中处理终端2为二级终端,比一级处理终端1a-1c高一级。每个处理终端都配有与之唯一对应的身份合牌3a-3d(对应关系如图1所示)。身份合牌可通过例如USB接口与处理终端连接,其中存储有代表所连接终端的唯一身份识别码,也就是说,用户只有持有相应身份合牌,才能操作某一对应的处理终端。该系统还包括管理服务器4。多个财务数据处理终端1a-1c、2等以及管理服务器4通过内部网络互相连接。当企业需要多层级上报财务数据时,可根据图1所示的系统,设置三级以上的处理终端,进行多层级扩展。

[0014] 二级终端2希望汇总财务数据时,例如二级终端2为人力资源汇总终端,希望汇总代表下属4S店的一级终端中生成的关于新晋销售人员培训花费的财务数据,二级终端2的用户将其对应的身份合牌3d与二级终端2连接,二级终端2读取身份合牌3d中保存的身份识别码D。确认当前用户有权限操作该二级终端2之后,二级终端2对该汇总代表下属4S店的一级终端中生成的关于新晋销售人员培训花费的财务数据的任务进行任务等级确认,例如此类数据并不重要、或对4S点后续规划有指导意义时,将其划分为一类任务;或企业并不希望4S店保存该数据,并且该数据汇总到二级终端2为止时,将其划分为二类任务;或二级终端2也仅仅是该数据的中转站,该数据最终将仅保存在三级终端中时,将其划分为三类任务等等。任务等级确认后,二级终端2将包括任务等级的新晋销售人员培训花费的财务数据接收请求和自身身份识别码D发送至管理服务器4。

[0015] 管理服务器4接收到该新晋销售人员培训花费的财务数据接收请求后,将该请求向所有一级终端广播(例如图1所示的1a-1c)。一级终端1a-1c接收到广播消息后,检查自身是否存储有所请求的财务数据,若有(例如图1所示的1a、1c存储有所请求的财务数据),待各自的操作用户将管理合牌3a、3c连接到一级终端1a、1c进行操作时,对用户进行提示,经用户操作后,一级终端1a将管理合牌3a中保存的身份识别码A连同自身存储的新晋销售人员培训花费的财务数据发送到管理服务器4,同样地,一级终端1c也将管理合牌3c中保存的身份识别码C连同自身存储的新晋销售人员培训花费的财务数据发送到管理服务器4。发送

完毕后,一级终端1a、1c根据新晋销售人员培训花费的财务数据接收请求中包含的任务等级,确定是否删除本机存储的财务数据。其中,当任务等级大于终端等级时,终端在将自身存储的财务数据发送到管理服务器4之后,自动将该财务数据删除;当任务等级小于等于终端等级时,继续保存该财务数据。这样可以防止财务数据存储在过多的终端中,并尽量在级别较高的终端中存储,减少了泄密的可能性。

[0016] 管理服务器4接收到一级终端1a、1c分别发送的新晋销售人员培训花费的财务数据和相应的身份识别码A、C后,根据财务数据发送方和接收方的身份识别码A、C、D,生成表示汇总代表下属4S店的一级终端中生成的关于新晋销售人员培训花费的财务数据的任务的任务密码E。该任务密码E根据以下的方式生成:对于每一终端,管理服务器4中都存储有与之对应的6位身份暗码,该身份暗码与身份识别码不同,仅存储在管理服务器4中,具有极强的保密性;管理服务器4根据任务所涉及的所有终端,读取所有相应身份暗码,确定身份暗码的数量n,生成位数为(6*n+8)位的任务初始码,其中该任务初始码从第1位开始,每6位都和某一终端的身份暗码相同,最后8位则为一串随机字符;对于(6*n+8)位的任务初始码,采用整体移位加密方式生成任务密码E,即将每位字符均向左或向右移动若干位,右边或左边空出的位数由左边或右边多出的字符补满。采用这种方式生成的任务密码E具有很强的保密性,并且管理服务器还可以从中解析出所有涉及的终端,方便后续任务操作。例如,当任务涉及终端1a、1c、2时,身份暗码例如分别为aaa111、ccc333、ddd444,数量为3,随机字符为e e e e 5 5 5 5 ,移位方式为向右移动5位,则生成的任务密码E为e5555aaa111ccc333ddd444eee,共26位。管理服务器4将一级终端1a、1c分别发送的新晋销售人员培训花费的财务数据设置为通过任务密码E才能读取,并将其与生成的任务密码E发送给二级终端2。

[0017] 二级终端2接收到管理服务器4发送的一级终端1a、1c的新晋销售人员培训花费的财务数据和生成的任务密码E后,将财务数据存储于终端内,将任务密码E存储到与二级终端2连接的身份合牌3d中。之后用户通过身份合牌3d连接到二级终端2后,二级终端2读取到身份合牌中存储的任务密码E后,用户才能读取或处理新晋销售人员培训花费的财务数据。这样,在后续进行操作时,即使不相干人士通过不法手段获知了二级终端2的身份识别码D,并仿造了存储有身份识别码D的伪身份合牌,但由于伪身份合牌中并未存储任务密码E,则不能读取或处理相应财务数据。对于每一个财务任务,均采用此类方式,可以有效防止财务数据被泄露或篡改。

[0018] 如图2所示,本发明所述的一种财务数据的内部网络安全传输方法,包括如下步骤:

[0019] S1,二级终端2希望汇总财务数据时,用户将其对应的身份合牌3d与其连接,读取身份合牌3d中保存的身份识别码D。确认当前用户有权限操作该二级终端2之后,二级终端2对该汇总该财务数据的任务进行任务等级确认。任务等级确认后,二级终端2将包括任务等级的财务数据接收请求和自身身份识别码D发送至管理服务器4。

[0020] S2,管理服务器4接收到该财务数据接收请求后,将该请求向所有一级终端广播(例如图1所示的1a-1c)。一级终端1a-1c接收到广播消息后,检查自身是否存储有所请求的财务数据,若有(例如图1所示的1a、1c存储有所请求的财务数据),待各自的操作用户将管理合牌3a、3c连接到一级终端1a、1c进行操作时,对用户进行提示,经用户操作后,一级终端

1a将管理合牌3a中保存的身份识别码A连同自身存储的财务数据发送到管理服务器4,同样地,一级终端1c也将管理合牌3c中保存的身份识别码C连同自身存储的财务数据发送到管理服务器4。发送完毕后,一级终端1a、1c根据财务数据接收请求中包含的任务等级,确定是否删除本机存储的财务数据。其中,当任务等级大于终端等级时,终端在将自身存储的财务数据发送到管理服务器4之后,自动将该财务数据删除;当任务等级小于等于终端等级时,继续保存该财务数据。

[0021] S3,管理服务器4接收到一级终端1a、1c分别发送的财务数据和相应的身份识别码A、C后,根据财务数据发送方和接收方的身份识别码A、C、D,生成表示汇总财务数据的任务的任务密码E。该任务密码E根据以下的方式生成:对于每一终端,管理服务器4中都存储有与之对应的6位身份暗码,该身份暗码与身份识别码不同,仅存储在管理服务器4中,具有极强的保密性;管理服务器4根据任务所涉及的所有终端,读取所有相应身份暗码,确定身份暗码的数量n,生成位数为(6*n+8)位的任务初始码,其中该任务初始码从第1位开始,每6位都和某一终端的身份暗码相同,最后8位则为一串随机字符;对于(6*n+8)位的任务初始码,采用整体移位加密方式生成任务密码E,即将每位字符均向左或向右移动若干位,右边或左边空出的位数由左边或右边多出的字符补满。管理服务器4将一级终端1a、1c分别发送的财务数据设置为通过任务密码E才能读取,并将其与生成的任务密码E发送给二级终端2。

[0022] S4,二级终端2接收到管理服务器4发送的一级终端1a、1c的财务数据和生成的任务密码E后,将财务数据存储于终端内,将任务密码E存储到与二级终端2连接的身份合牌3d中。之后用户通过身份合牌3d连接到二级终端2后,二级终端2读取到身份合牌中存储的任务密码E后,用户才能读取或处理新晋销售人员培训花费的财务数据。

[0023] 以上实施例仅用于说明本发明,而并非对本发明的限制,有关技术领域的普通技术人员,在不脱离本发明的精神和范围的情况下,还可以做出各种变化和变型,因此所有等同的技术方案也属于本发明的范畴,本发明的专利保护范围应由权利要求限定。

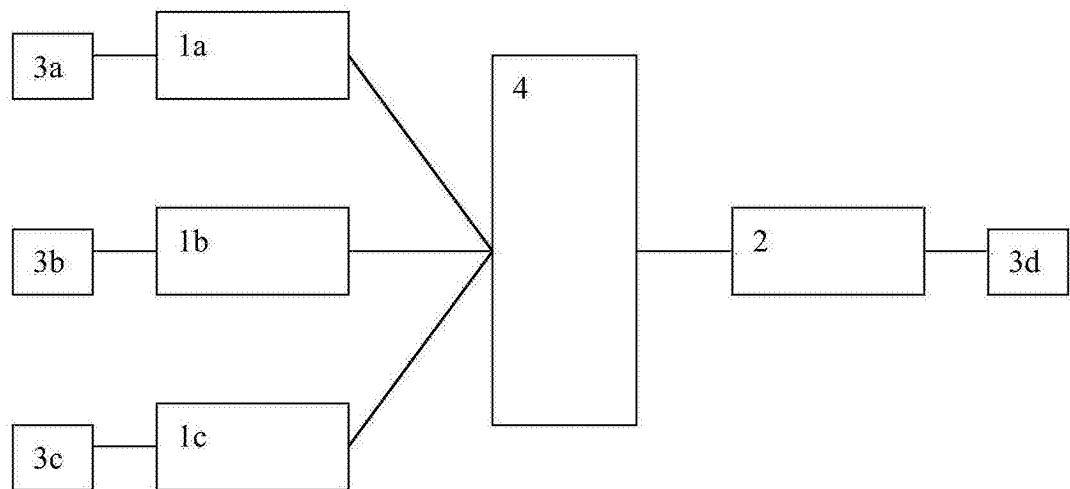


图1

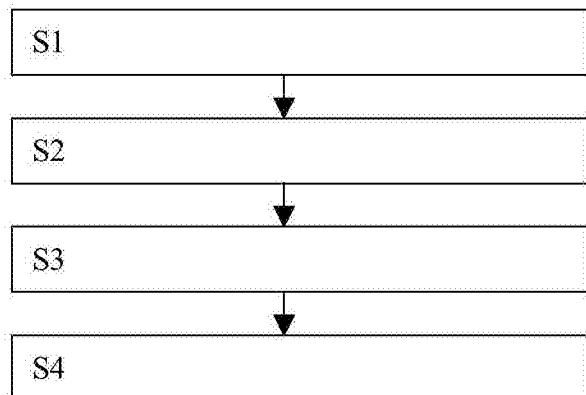


图2